Turvallisuusluokka II:n vaatimusten mukainen tila ja tietoverkko

Ylinen, Ari

2009 Laurea Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Turvallisuusluokka II:n vaatimusten mukainen tila ja tietoverkko

Ari Ylinen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Marraskuu, 2009

Laurea-ammattikorkeakoulu
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma
Yritysten tietoverkot

Tiivistelmä

Ari Ylinen

Turvallisuusluokka II:n vaatimusten mukainen tila ja tietoverkko

Vuosi 2009 Sivumäärä 41

Tutkimuksen tarkoituksena oli selvittää sellaisen tilan tietoverkon vaatimuksia ja käytännön toteuttamisvaihtoehtoja, joka luokitellaan turvallisuusluokka II:n (salainen) mukaan. Työssä keskityttiin tutkimaan, mitä asioita verkon sekä tilan suunnittelussa ja rakentamisessa tulee ottaa huomioon niin, että turvallisuusluokka II:n vaatimukset tulevat täytettyä. Työn taustalla on Leppävaaran Laureaan rakennettava turvallisuuslaboratorio. Lisäksi työssä tutkittiin miten Linuxia voisi hyödyntää tilaan tulevaa tiedostopalvelinta varten.

Tutkimusmenetelmänä työssä käytettiin konstruktiivista eli suunnittelutieteellistä tutkimustapaa. Tutkimuksessa käytettiin tiedonlähteinä pääosin alaan liittyviä luotettavia ja ajan tasalla olevia kirjoja ja Internet-lähteitä. Turvallisuuslaboratorioon liittyvien asioiden lähteenä olivat keskustelut Laurean yliopettaja Jyri Rajamäen kanssa. Linuxia käsittelevässä osuudessa käytettiin lähteenä myös omalla Ubuntu-työasemalla suoritettuja testejä.

Tutkimuksessa selvisi, että turvallisuusluokitellun tietoaineiston käsittelystä on kaikissa luokissa (I-IV) tarkasti säädetty käytännöt, joita tulee noudattaa aineiston käsittelyssä. Määrittelyt kattavat asiakirjan koko elinkaaren luomisesta tuhoamiseen. Myös tilan, jossa käsitellään luokiteltua materiaalia, sekä tilassa olevien työasemien, palvelimien ja verkkojen tulee tukea niitä vaatimuksia, jotka turvallisuusluokittelu asettaa turvaluokitellun materiaalin käsittelyyn.

Tutkimuksen perusteella voidaan sanoa, että tilan suunnittelussa tulee olla erityisen tarkka ja tulee kohta kohdalta käydä läpi vaatimukset, että tilasta tulee määritysten mukainen. Henkilökunnan kouluttamiseen ja ohjeistamiseen tulee kiinnittää suurin huomio, koska turvaluokittelu vaatii henkilökunnalta paljon rutiineja päivittäisessä toiminnassa. Erittäin tärkeää olisi myös jollain tavoin valvoa, että henkilökunta käyttäytyy turvaluokittelun vaatiman tietoturvan vaatimusten mukaan.

Asiasanat turvallisuusluokittelu, turvallisuusluokka II, Linux

Laurea University of Applied Sciences
Laurea Leppävaara
Information Technology Programme
Information Systems and Data Communication

Abstract

Ari Ylinen

Facility and network for measuring up to the requirements of Security Classification II

Year 2009 Pages 41

The purpose of the thesis was to define requirements and actual realization alternatives for a network that measures up the requirements of Security Classification II (classified). The main focus of the thesis was to define the main points that should be taken into consideration when planning and building the network so that the requirements of the Security Classification II would be fulfilled. The background for the thesis was the construction of the SID Security Management Laboratory at Laurea University of Applied Sciences. The thesis also included a study on how Linux could be put into use in building a file server for the Security Lab.

The research method used was constructive. The sources of information used in the research were books and Internet sources that are current and reliable. All the information about the Security Lab was obtained from interviews with Jyri Rajamäki, a principal lecturer at Laurea. The section that studies Linux was partly based on writer's experiences and tests with desktop Ubuntu.

The research of the security classification showed that there are strict rules about processing documents that are under security classification. The determination covers the whole life cycle of a document from creation to deletion. The facility, workstations, servers and the network where classified material is processed need to fulfil the requirements of the security classifications.

According to the research the planning of the facility needs to be accurate so that the requirements will be fulfilled. The training of the staff is the most important factor because the daily tasks require a lot of routines from the staff. It is also important to monitor that the staff follows the rules of the security classifications.

Key words security classification, security classification II, Linux

Sisällys

1 Johdanto

Opinnäytetyössä tutkitaan sellaisen tilan tietoverkon vaatimuksia ja käytännön toteuttamisvaihtoehtoja, joka luokitellaan turvallisuusluokka II:n (salainen) mukaan. Työssä keskitytään tutkimaan mitä asioita verkon suunnittelussa ja rakentamisessa tulee ottaa huomioon niin, että turvallisuusluokka II:n vaatimukset tulevat täytettyä. Turvallisuusluokittelun tuomien vaatimusten lisäksi työssä tutkitaan Linuxin ja vapaiden ohjelmistojen tarjoamia mahdollisuuksia edellä mainitun kaltaisen tietoverkon tiedostopalvelimen toteuttamiseksi.

Opinnäytetyön taustalla on Laureaan perustettava SID Security Management Laboratory, jonka on tarkoitus valmistua kesällä 2009. SID Security Management Laboratory, josta käytetään yleisesti nimeä turvalabra, mahdollistaa eri hankkeisiin liittyvät asennukset osallistujayrityksistä turvaluokitusten mukaisesti. Labran toimintaan tulee liittymään myös Opetusministeriön Laurealle antama tehtävä koordinoida korkeakoulujen turvallisuutta kehittävää hanketta yhdessä muiden alan korkeakoulujen (mm. Maanpuolustuskorkeakoulu, Pelastusopisto sekä Poliisiammattikorkeakoulu) kanssa.

Opinnäytetyössä pääpaino tulee olemaan turvallisuusluokitusten vaatimusten selvittämisessä sekä erilaisten ratkaisujen tutkimisessa, joilla vaatimukset saadaan täytettyä. Opinnäytetyön alussa selvitetään turvalabran tausta ja tarkoitus sekä käsitellään tutkimusmenetelmiä. Seuraavaksi käsitellään turvallisuusluokituksia yleisesti sekä tarkemmin turvallisuusluokka II:ta. Tämän jälkeen tutkitaan tilan tietoverkon vaatimuksia ja käytännön toteuttamisvaihtoehtoja turvallisuusluokka II:n kannalta, joka on tässä työssä tutkimusongelmana.

Turvallisuusluokittelujen käsittelyn jälkeen työssä tutkitaan, mitä valmiita ratkaisuja Linux sekä muut vapaat ohjelmat tarjoavat turvallisuusluokittelun vaatimusten mukaisen tilan ja sen tietoverkon tiedostopalvelimen rakentamiseen.

1.1 Tutkimusongelma

Opinnäytetyön tavoitteena on tutkia turvallisuusluokittelua ja erityisesti turvallisuusluokka II:ta. Työn lähtökohtana on selvittää mitä vaaditaan tilalta, jossa tullaan käsittelemään tietoaineistoa, joka luokitellaan turvallisuusluokka II:n mukaan. Työssä käydään läpi käytännön toteuttamisvaihtoehtoja turvallisuusluokittelun vaatimusten täyttämiseksi. Tilan lisäksi työssä selvitetään tilaan tulevan tietoverkon käytännön toteuttamisvaihtoehtoja sekä sitä, mitä tulee ottaa huomioon tilan käyttäjien kouluttamisessa. Lisäksi työssä tutkitaan Linuxin ja muiden vapaiden ohjelmien tarjoamia etuja sekä mahdollisuuksia tiedostopalvelimen toteuttamiseen turvallisessa ympäristössä.

2 Taustaa

2.1 Laurea SID

LaureaSID (Service, Innovation, Design) on palveluliiketoimintaan keskittynyt Leppävaarassa sijaitseva Laurea-ammattikorkeakoulun yksikkö. Opiskelu LaureaSID:ssä pohjautuu Learning by Developing (LbD) -toimintamalliin. (LaureaSID. 2009.)

LbD on kehittämispohjaista oppimista, jossa oppimisprosessi on muotoiltu tutkimis- ja kehittämisprosessiksi. Käytännössä Lbd-toimintamallissa opinnot suoritetaan yhteistyössä yritysten ja organisaatioiden kanssa erilaisissa käytännön projekteissa, joissa opitaan tekemällä. Kumppanuusperiaate on projektien perusta, mikä tarkoittaa sitä, että opiskelijat, opettajat sekä yhteistyökumppanit ovat tasavertaisia toimijoita. LbD-toimintamalli antaa opiskelijalle käytännön tasolla mahdollisuuden kehittää, keksiä sekä luoda uutta, mutta samalla se myös edellyttää opiskelijalta aktiivisuutta sekä vastuunottokykyä. (LaureaSID 2009.)

LaureaSID:ssä voi opiskella niin suomen kuin englannin kielellä AMK-tutkinnon, sekä ylemmän AMK-tutkinnon. Suomenkieliset AMK-koulutusohjelmat ovat: Hotelli- ja ravintola-alan liikkeenjohdon koulutusohjelma, Liiketalouden koulutusohjelma, Palvelujen tuottamisen ja johtamisen koulutusohjelma, Tietojenkäsittelyn koulutusohjelma sekä Turvallisuusalan koulutusohjelma. Englanninkieliset AMK- koulutusohjelmat ovat: Business Management sekä Business Information Technology. Ylemmän AMK:n koulutusohjelmat ovat: Tietojärjestelmäosaamisen koulutusohjelma, Turvallisuusosaamisen koulutusohjelma, Palveluliiketoiminnan koulutusohjelma, Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma sekä Degree Program in Service Innovation and Design. (LaureaSID 2009.)

2.2 LaureaSID Labs

Laureassa toimii useita eri alojen tutkimus- ja kehitysympäristöjä, joissa yhdistyy sekä opetus että tutkimus- ja kehitystoiminta. Näistä kahdeksasta Leppävaarassa sijaitsevasta tutkimus- ja kehitysympäristöstä käytetään nimitystä LaureaSID Labs, ja ne tarjoavat palveluja sekä yhteistyömahdollisuuksia suurkaupunkialueella. LaureaSID Labsissa eri alojen asiantuntijoiden, opiskelijoiden, opettajien, Laurean yhteistyökumppaneiden ja asiakkaiden yhteistyönä syntyy uutta osaamista. Eri labrat tarjoavat useille opiskelijoille myös työharjoittelupaikan tai vaikkapa aiheen opinnäytetyölle. SID Labsin projektien kautta voi hankkia myös opintopisteitä tutkimus- ja kehitysympäristössä. (LaureaSID Labs 2009.)

Kaikki SID Labsit tekevät läheistä yhteistyötä eri yritysten ja organisaatioiden kanssa. LaureaSID Labsien kahdeksasta tutkimus- ja kehitysympäristöstä osa on vielä kehitysvaiheessa. Labrojen nimet sekä osaamisalueet ovat:

- SIDlab Business
  Markkinointi, palveluliiketoiminta ja yhteiskuntavastuu

- SIDlab Balance
  Talouden ohjaus

- SIDlab Networks
  Web2, verkkoteknologia, jaettu laskenta ja sisätilapaikannus

- SIDlab Red
  Laurean ja IT-palveluiden kehittäminen, innovatiiviset ohjelmistoratkaisut, turvallisuusjohtaminen ja riskienhallinta

- SIDlab Neon
  Tietojärjestelmät, tiedon louhinta, avoimen lähdekoodin ohjelmistot, Oracle Academy ja Sun Academic Initiative (SAI) for Java

- SIDlab Bar Laurea
  Palveluliiketoiminnan ja palvelujärjestelmien tutkimus- ja kehittämishankkeet, tuotetestaukset, vaihtoehtoiset tuotantotavat, reseptiikan kehittäminen, järjestelmätestaukset, perehdyttämis- ja koulutusmateriaalit, markkinointimateriaalit

- SIDlab Security
  Turvallisuus

- SIDlab International

(LaureaSID Labs 2009.)

2.3 Laureasta koulutuksen laatuyksikkö

Korkeakoulujen arviointineuvosto (KKA) on nimennyt Laurea-ammattikorkeakoulun turvallisuusalan koulutusohjelman koulutuksen laatuyksiköksi vuosille 2008–2009. Ammattikorkeakoulutuksen laadun kehittämiseen ja näkyvyyden parantamiseen tähtäävässä laatuyksikköarvioinnissa arvioitiin yksiköiden toimintaa seuraavien kohteiden osalta: koulutusyksikön toiminnan kuvaus ja nivoutuminen ammattikorkeakoulun strategiaan sekä keskeisiin pedagogisiin linjauksiin, koulutusyksikön toiminnan suunnittelu, toteutus, arviointi ja kehittäminen sekä koulutusyksikön toiminnan tulokset suhteessa sille asetettuihin tavoitteisiin. (Laureasta koulutuksen laatuyksikkö 2008 – 2009.)

Korkeakoulujen arviointineuvostolla oli 20 kirjallista esitystä koulutuksen laatuyksiköksi eri ammattikorkeakouluista. Laurean turvallisuusalan koulutusohjelman lisäksi koulutuksen laatuyksiköksi valittiin myös Haaga-Helia ammattikorkeakoulu, johdon assistenttityön ja kielten koulutusohjelma; Rovaniemen ammattikorkeakoulu, hoitotyön koulutusohjelma; Savonia-ammattikorkeakoulu, yrittäjyysosaamisen kehittäminen maatalouden koulutusohjelmassa ja Turun ammattikorkeakoulu, rakennustekniikan koulutusohjelma. (Laureasta koulutuksen laatuyksikkö 2008 – 2009.)

Vuonna 1998 Laurean turvallisuusala aloitti yksityiseen turvallisuuteen suuntautuvana liiketalouden tradenomikoulutuksena. Vuosien aikana se on saanut rinnalleen osaamista laajentavina tietoturvallisuuden, riskienhallinnan ja kansainvälisen turvallisuusjohtamisen erikoistumisopinnot sekä ylempään ammattikorkeakoulututkintoon johtavan turvallisuusosaamisen koulutusohjelman. Syksyllä 2008 turvallisuusalan koulutusohjelma sai myös opetusministeriön toimeksiannon korkeakouluturvallisuuden kehittämiseksi yhdessä muiden alan korkeakoulujen kanssa. (Laureasta koulutuksen laatuyksikkö 2008 – 2009.)

2.4 SID Security Management Laboratory

Koulutuksen laatuyksiköksi valituille yksiköille kohdennetaan opetusministeriön tuloksellisuusrahaa (Laureasta koulutuksen laatuyksikkö 2008 – 2009). Kyseisen rahoituksen turvin on Laureaan päätetty perustaa SID Security Management Laboratory. SID Security Management Laboratory, josta käytetään myös nimeä turvalabra, mahdollistaa eri hankkeisiin liittyvät asennukset osallistujayrityksistä turvallisuusluokitusten mukaisesti. Labran toiminta tulee liittymään myös toimeksiantoon korkeakouluturvallisuuden kehittämiseen yhdessä alan muiden korkea-

koulujen kanssa. Muihin alan korkeakouluihin kuuluu Maanpuolustuskorkeakoulu, Pelastusopisto sekä Poliisiammattikorkeakoulu.

SID Security Management Laboratory sisältää yleisen ja salaisen puolen. Salainen puoli tullaan luokittelemaan salaiseksi turvallisuusluokka II:n mukaan. Turvallisuusluokittelusta sekä erityisesti turvallisuusluokka II:sta kerrotaan tarkemmin luvussa 4. Turvalabra tulee sijoittumaan Leppävaaran Laureaan siten, että salainen puoli tulee alimmassa kerroksessa olevaan väestönsuojaan, ja yleinen puoli tulee vieressä oleviin tiloihin, missä ennen oli kuntosali.

Turvalabran salaiselle puolelle tullaan rakentamaan Linux-verkko, joka on täysin eristetty muista verkoista. Labran yleisen puolen tiloista/tiloihin tulee pääsy Laurean verkkoon, sillä siitä tulee myös joidenkin opettajien työtila. SID Security Management Laboratoryn yleinen puoli rakennetaan ensin ja sen on tarkoitus valmistua kevään 2009 aikana. Labran salaisen puolen pitäisi valmistua kesällä 2009.

SID Security Management Laboratoryn yhteyshenkilöitä ovat turvan Jouni Viitanen sekä Juha Leppänen.

3 Menetelmät

3.1 Tutkimusmenetelmät

Tutkimusmenetelmänä työssä käytetään konstruktiivista eli suunnittelutieteellistä tutkimusmenetelmää. Edellä mainittu tutkimustapa sopii tutkimusmenetelmäksi hyvin, koska työssä on tavoitteena luoda uutta tietoa soveltaen tuloksia perustutkimuksista sekä tunnetuista asioista. (Järvinen & Järvinen 2004, 103.) Työssä tullaan turvaluokitellun aineiston käsittelyvaatimusten pohjalta selvittämään, mitä asioita tulee ottaa huomioon rakennettaessa verkkoa tilaan, jossa käsitellään ja luodaan luokiteltavaksi vaadittavaa tietoa.

Konstruktiiviselle tutkimustieteelle on ominaista, että tutkimuskysymys sisältää sanoja rakentaa, muuttaa, parantaa, vahvistaa, laajentaa, korjata, sovittaa jne. Van Aken (2004) korostaa konstruktion sekä parantamisen käyttävän samanlaista lähestymistapaa ja tuottavan teknologiseksi säännöksi kutsutun samanlaisen tuloksen.

3.2 Tiedon kerääminen

Tietoa kerätessä käytettiin alaan ja työn aiheeseen liittyvää kirjallisuutta sekä internetistä ja siellä olevista tietokannoista löytyviä luotettavia aineistoja. Turvalaboratorioon liittyvän tiedon keräämiseen tulen käyttämään lisäksi myös keskusteluja/haastatteluja, joita olen käynyt Laurean yliopettaja Jyri Rajamäen kanssa.

Alan kirjallisuudessa on yleensä perusasiat hyvin kunnossa, mutta tieto ei välttämättä pysy kovinkaan hyvin ajantasalla, koska tietotekniikka kehittyy koko ajan suurin harppauksin. Tästä syystä on usein kannattavampaa käyttää internetistä löytyvää uudempaa ja ajantasaisempaa tietoa, kuin jo ehkä vanhentunutta painettua tietoa. Internetistä löytyvä tieto on myös helpommin ja nopeammin löydettävissä.

Internetistä tietoa etsiessä on hyvä suhtautua tietoon kriittisesti, koska sieltä löytyy myös runsaasti epäpätevää ja tarkistamatonta tietoa. Tästä syystä kannattaakin käyttää tunnettuja sekä luotettavia sivustoja lähteenä, eikä esimerkiksi keskustelupalstoja, jonne kuka tahansa voi kirjoittaa oman mielipiteensä ilman perusteluja.

Kerätyn tiedon avulla pyrin selvittämään kattavasti turvallisuusluokittelun taustat ja säännöt, sekä tutkimaan, mitä vaatimuksia ne tuovat rakennettavalle tilalle sekä verkolle.

3.3 Rajaukset

Työssä keskitytään turvallisuusluokituksista erityisesti turvallisuusluokka II:een sekä siihen, minkälaisia vaatimuksia turvallisuusluokittelu tuottaa tilan ja verkon käytännön toteutukselle. Työssä ei tulla käsittelemään kovin tarkasti verkon rakentamista, dokumentointia, palveluita tai testausta eikä mitään muitakaan asioita, jotka eivät ole turvallisuusluokittelun kannalta olennaisia.

4 Turvallisuusluokittelu

4.1 Vahti

VAHTI eli valtiohallinnon tietoturvallisuuden johtoryhmä on valtiovarainministeriön asettama ja se on asetettu hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. Suomessa valtiohallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset käsittelee VAHTI. Lisäksi VAHTI ohjaa valtiohallinnon tietoturvatoimenpiteitä. VAHTI toimii yhteistyö-, valmistelu- ja koordinaatioelimenä hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaaville hallinnon organisaatioille, sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä. Tietoturvallisuutta kehittämällä VAHTI tavoittelee valtiohallinnon toimintojen luotettavuuden, jatkuvuuden, laadun, riskienhallinnan ja varautumisen parantamista sekä tietoturvallisuuden kiinteäksi saattamisen edistämistä osana hallinnon toimintaa, johtamista ja tulosohjausta. (Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI 2009.)

Kaikki valtiohallinnan tietoturvallisuuden osa-alueet kuuluvat VAHTIn toimialaan:

- hallinnollinen tietoturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus.

(Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI 2009.)

4.2 Suojaustasot ja turvallisuusluokitukset

Valtiohallinnon viranomaisten tietoturvallisuustoimenpiteillä pyritään turvaamaan asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen saatavuus, käytettävyys, suoja, eheys ja laatu. Jotta tietoturvallisuus toteutuu, on valtiohallinnon viranomaisten huolehdittava toimenpiteistä asiakirjojen salassapidon varmistamiseksi, asiattoman pääsyn estämiseksi tietojärjestelmiin ja tietojen saannin ja käytettävyyden turvaamisesta eri tilanteissa, toimitilojen turvallisuudesta sekä henkilöstön luotettavuudesta ja asianmukaisten ohjeiden ja koulutuksen antamisesta henkilöstölle ja muille tietoaineistojen käsittelyyn liittyviä tehtäviä hoitaville. Jos viranomaisen päätöksellä asiakirja on luokiteltu tietoturvallisuuden toteuttamiseksi, asiakirjan käsittelyssä tulee noudattaa turvallisuusluokituksesta säädettyjä perusteita. Valtiohallinnon viranomainen on vastuussa siitä, että sen laatimien tai saamien luokiteltujen asiakirjojen käsittelyssä noudatetaan luokittelua vastaavia turvallisuustoimenpiteitä. (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa. 2008.)

Tietoturvallisuustoimenpiteiden suunnittelussa ja toteutuksessa on otettava huomioon, että sen tulee kattaa kaikki asiakirjan käsittelyvaiheet niiden laatimisesta tai vastaanottamisesta arkistointiin tai hävittämiseen mukaan lukien asiakirjan luovuttaminen ja siirtäminen sekä käsittelyn valvonta. (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa 2008.) ”Turvallisuusluokittelulla osoitetaan, millaisia tietoturvatoimenpiteitä edellytetään tietoaineistojen ja asiakirjojen käsittelyltä silloin, kun aineisto sisältää sellaista salassa pidettävää tietoa, jonka oikeudeton paljastuminen voi aiheuttaa vahinkoa kansainvälisille suhteille, val-

tion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille” (Tietoaineistojen turvallinen käsittely 2008).

Tietoa, joka vaatii salassapitoa, voi esiintyä monessa eri muodossa. Viranomaisten asiakirjat, valmistelussa olevat asiakirjat ja tietoaineistot voivat sisältää salassa pidettävää tietoa. Julkisuuslaissa asiakirja käsitteenä on laaja ja se kattaa myös erilaiset tekniset tallenteet. Salassa pidettävää tietoa voidaan välittää erilaisin viestinnän keinoin, kuten sähköpostin, puhe- ja videoyhteyksien avulla. Myös useat tietojärjestelmät käsittelevät salassa pidettävää tietoa. Käyttäjän tulee kuitenkin tiedostaa kaikissa tilanteissa salassa pidettävän tiedon käsittelyyn liittyvät vaatimukset. (Tietoaineistojen turvallinen käsittely 2008.)

Salattava tietoaineisto on joko turvallisuusluokiteltua tai muuta suojattavaa tietoa sisältävää. Turvallisuusluokiteltu aineisto on aina salassa pidettävää. Kaikki muu suojattava aineisto voi olla salassa pidettävää, harkinnanvaraisesti suojattavaa tai käyttötarkoitussidonnaista. Kaikkea salassa pidettävää tietoaineistoa käsitellään suojaustasojen avulla. Suojaustasolla määritellään, millaisia tietoturvatoimenpiteitä tietoaineiston ja asiakirjojen käsittelyltä vaaditaan. (Tietoaineistojen turvallinen käsittely 2008.)

Salassa pidettävien asiakirjojen tai niihin sisätyvien tietojen luokittelu voidaan toteuttaa sen mukaan, minkälaista tietoturvallisuutta koskevia vaatimuksia niiden käsittelyssä on tarpeen noudattaa. Luokittelun voi suorittaa myös kohdistamalla tietoturvallisuutta koskevat vaatimukset vain sellaisiin asiakirjan käsittelyvaiheisiin, joissa erityistoimenpiteet ovat suojattavan edun vuoksi tarpeen. Sellaisiin osiin asiakirjan luokitusta ei saa ulottaa, joissa käsittelyvaatimusten noudattaminen ei suojattavan edun vuoksi ole tarpeen. (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa 2008.)

Kuvio 1. Salassa pidettävää tietoa sisältävän asiakirjan tai tietovarannon rakenne. (Tietoaineistojen turvallinen käsittely 2008.)

Salassa pidettävät asiakirjat jaetaan seuraaviin luokkiin:

1. Suojaustaso I ”erittäin salainen”, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille;

2. Suojaustaso II ”salainen”, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille;

3. Suojaustaso III ”luottamuksellinen”, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetuille yleisille ja yksityisille eduille;

4. Suojaustaso IV ”käyttö rajoitettu”, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetuille yleiselle tai yksityiselle edulle.

Suojaustasoon IV voidaan luokitella muukin kuin salassa pidettäväksi säädetty asiakirja, jos lain mukaan asiakirjan luovuttaminen on viranomaisen harkinnassa tai asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen ja jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä. (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa. 2008.)

Suojaustason kertovan merkinnän yhteyteen voidaan merkitä myös tieto asiakirjan salassapidosta. Suojaustasomerkintä on tehtävä asiakirjaan selvästi ja oikein, ja luokitus säilytettävä vain niin pitkään, kun se tietojen suojan vuoksi on tarpeellista. Jos asiakirjaan merkintöjen tekeminen tai muuttaminen ei ole teknisesti mahdollista tai jos luokkaa vastaavat käsittelyvaatimukset ovat tarpeen vain lyhyen ajan, voidaan vaadittavat merkinnät tehdä asiakirjaan liitettävään erilliseen asiakirjaan. Kun asiakirjan luokitukselle ei ole enää perusteita lain mukaan tai luokitusta on tarpeen muuttaa, on asiakirjaan tehtävä asianmukainen merkintä luokituksen poistamisesta, jollei luokituksen muuttaminen tai poistaminen ole muutoin mahdollista asiakirjaa vahingoittamatta. Toiselta valtiohallinnan viranomaiselta saadun suojaustasoa I-III edellyttävän asiakirjan luokitusmerkintää ei saa muuttaa ilman asiakirjan antaneen viranomaisen lupaa. (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa. 2008.)

Asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tehdä erityinen turvallisuusluokitusmerkintä, jos asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muille yleisille eduille. Turvallisuusluokiteltua aineistoa käsitellään suojaustasoille asetettujen vaatimusten mukaisesti.

Turvallisuusluokitusmerkintä tehdään seuraavasti:

1. suojaustasoon I kuuluvaan asiakirjaan merkinnällä ”erittäin salainen”;

2. suojaustasoon II kuuluvaan asiakirjaan merkinnällä ”salainen”;

3. suojaustasoon III kuuluvaan asiakirjaan merkinnällä ”luottamuksellinen”;

4. suojaustasoon IV kuuluvaan asiakirjaan merkinnällä ”käyttö rajoitettu”.

Turvallisuusluokitusmerkintää ei saa käyttää muissa kuin yllä mainituissa tapauksissa, jollei asiakirja liity kansainväliseen yhteistyöhön tai kuulu kansainvälisistä tietoturvallisuusvelvoitteista annetun lain soveltamisalan piiriin. (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa. 2008.)

Turvallisuusluokitusten vastaavuus kansainvälisiä velvoitteita toteuttaessa on seuraava: turvallisuusluokitusmerkintää ”erittäin salainen” vastaa kansainvälisten sopimusten luokka ”top secret” tai sitä vastaava muun kielinen ilmaisu; merkintää ”salainen” vastaa ”secret” tai sitä vastaava muun kielinen ilmaisu; merkintää ”luottamuksellinen” vastaa ”confidential” tai sitä vastaava muun kielinen ilmaisu ja merkintää ”käyttö rajoitettu” sopimusten luokkaa ”restricted” tai muu sitä vastaava ilmaisu. (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa. 2008.)

Kohde	Turvallisuusluokka I	Turvallisuusluokka II	Turvallisuusluokka III	Turvallisuusluokka IV
Suomi	ERITTÄIN SALAINEN	SALAINEN	LUOTTAMUK-SELLINEN	KÄYTTÖ RAJOITETTU
EU	Très secret UE/ EU Top Secret	Secret UE	Confidentiel UE	Restreint UE
NATO	Cosmic Top Secret	NATO Secret	NATO Confidential	NATO Restricted NATO Unclassified

Kuva 2. Kansainvälisten järjestöjen ja Suomen turvallisuusluokitusten vastaavuus. (Tietoaineistojen turvallinen käsittely. 2008.)

Valtiohallinnon viranomainen on vastuussa siitä, että asiakirjojen laadinnassa tulee toteuttaa mahdollisuuksien mukaan sellaisia asiakirjan rakenteita, joiden avulla voidaan toteuttaa samanaikaisesti asiakirjan julkisuus, sekä siihen sisältyvien salassa pidettävien tietojen suoja. Salassa pidettävien asiakirjojen käsittelyssä asianmukaisten toimenpiteiden on toteuduttava seuraavasti:

1. Asiakirjojen tietojenkäsittely- ja säilytystilat tulee olla riittävän valvottuja ja suojattuja.

2. Tietojärjestelmiin pääsyn tulee olla valvottua, sekä luvaton tunkeutuminen niihin tulee olla estettynä käytettävissä olevin keinoin.

3. Asiakirjoja saa käyttää, muuttaa ja muutoin käsitellä vain ne, joiden tehtäviin asian käsittely kuuluu. Käyttöoikeudet tulee myös rajata asianmukaisesti ja käyttöä pitää valvoa riittävästi.

4. Asiakirjoista tietoja saavat luovuttaa vain ne, joiden tehtäviin siitä huolehtiminen kuuluu.

5. Tietoverkoissa siirrettävä tieto tulee salata tarpeen mukaan. (Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa. 2008.)

4.3 Turvallisuusluokka II

Turvallisuusluokitellun tietoaineiston käsittelyssä käytetään vastaavien suojaustasojen käsittelyohjeita, jolloin turvallisuusluokka II:n mukaan luokiteltua aineistoa käsitellään suojaustaso II:n mukaan. Suojaustaso II:n käsittelyvaatimukset ovat seuraavat:

4.3.1 Elinkaarta koskevat vaatimukset

Elinkaarella tarkoitetaan annettujen vaatimusten noudattamista koko elinkaaren ajan, luomisesta tuhoamiseen.

- Suojauskohtaiset vaatimukset tulee huomioida koko elinkaaren ajan.
- Riittävät asiakirjan yksilöimiseen liittyvät tunnisteet tulee käydä ilmi asiakirjasta
- Asiakirjoja tulee käsitellä huolella siten, että salassa pidettävään tietoon pääsevät käsiksi vain ne, joilla on siihen oikeus. Erityisesti sellaisissa tilanteissa kun samassa tilassa on henkilöitä, joilla ei ole oikeutta salattuun tietoon, tulee asiakirjojen suojaaminen varmistaa.
- Kansainvälisten asiakirjojen kohdalla noudatetaan kansainvälisiä sopimuksia, jos mahdollista. Muutoin noudatetaan Suomen lakia.
- Asiakirjojen käsittelyvaatimuksia tulee noudattaa riippumatta siitä, missä muodossa tieto on tallennettu tai esitetty.
- Asiakirjoja tulee käsitellä arkistointisuunnitelman mukaisesti.
- Asiakirjoja ei saa jättää ilman valvontaa kun poistutaan työtilasta.
- Käsitellessä asiakirjoja tulee ottaa huomioon käsittely-ympäristölle asetetut luokkakohtaiset vaatimukset.
- Asiakirjojen käsittelyssä tulee ottaa huomioon henkilöstöturvallisuudelle asetetut vaatimukset, kuten käsittelyoikeuden edellytykset ja käsittelysääntöjen osaaminen.
- Asiakirjojen käsittelyä tulee välttää työpaikan ulkopuolella. Mikäli työtehtävät sitä kuitenkin edellyttävät, tulee asiakirjoja käsitellä tässä ohjeessa annettujen periaatteiden ja vaatimusten mukaisesti.
- Asiakirjoihin tutustuneista tulee jäädä täydellinen, kopiokohtainen jälki, joka mahdollistaa asiakirjan ja siitä otettujen kopioiden seurannan suojaustarvetta edellyttävältä ajalta. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.2 Asiakirjojen luonti ja vastaanotto

- Tietoaineistoa kerättäessä, luovutettaessa sekä asiakirjaa valmisteltaessa ja luotaessa on huomioitava asiakirjan julkisuudesta ja salassa pidosta annettu lainsäädäntö, arkistonmuodostussuunnitelman vaatimukset sekä viranomaisten antamat ohjeet
- Valmisteltaessa tulee huomioida, että aineistoa tulee koko prosessin ajan käsitellä ympäristössä, jossa vain käyttöoikeuden omaavat pääsevät aineistoon käsiksi.
- Tietoaineistoa valmisteltaessa tulee mahdollisuuksien mukaan eri käsittelyluokkiin kuuluvat tiedot esittää eri asiakirjoissa.
- Asiakirja on rekisteröitävä tai muulla tavoin hallittava.
- Jos Suomea sitovassa sopimuksessa määrätään tai suomen laki edellyttää, tulee turvallisuusluokitellut asiakirjat leimata vastaavilla kotimaisilla turvallisuusluokkaa osoittavilla leimoilla.
- Tietojärjestelmissä, jotka sisältävät salassa pidettävää tietoa, tulee tiedon laatijan ja käsittelijän varmistua, ettei ulkopuolisilla ole pääsyä tietoon ja että tiedon käsittely tapahtuu sallitussa ympäristössä, jossa vain oikeutetuilla henkilöillä on käsittelyoikeus.
- Tietojärjestelmät, jotka automaattisesti tuottavat tietoa, kuten valvonta-, loki- tai muuta salassa pidettävää tietoa, tulee käsittelijän varmistua myös omasta oikeudesta tietoon. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.3 Asiakirjojen luokittelu ja merkintä

Luokittelulla tarkoitetaan toimenpiteitä, joita tarvitaan asiakirjan tai tiedon suojaustason määrittelyssä. Merkinnällä tarkoitetaan asiakirjaan tulevan suojaustason tai turvallisuusluokkaa osoittavan leiman tekemistä.

- Salassa pidettävät asiakirjat on luokiteltava.
- Henkilön, joka antaa asiaan liittyvän toimeksiannon tai ensimmäisen kerran luo tiedon, tulee myös luokitella tieto.
- Asiakirjan laatija, ensimmäinen vastaanottaja tai henkilö, jolla on oikeus päättää tiedon käsittelystä ja käytöstä, tekee merkinnän käsittelyluokasta.
- Asiakirjan allekirjoittaja vahvistaa luokittelun manuaalisella tai sähköisellä allekirjoituksellaan.
- Asiakirjat merkitään osien ylintä suojaustasoa vastaavalla leimalla. Asiakirjojen laadinnassa suositellaan, että eri turvallisuusluokkiin kuuluvat tiedot esitetään omissa asiakirjoissa.
- Salassa pidettäviin asiakirjoihin tulee laittaa asianomaiset leimat.
- Leima tulee sijoittaa ensimmäisen sivun oikeaan yläkulmaan.

- Leima suositellaan sijoitettavan myös asiakirjan muille sivuille.
- Leiman tulee olla väriltään punainen.
- Suositeltavaa on, että käytetään leimaa, joka sivulla tai punaisella poikkiviivalla merkittyä paperia tai vastaavan merkinnän toteuttavaa tulostustapaa.
- Asiakirjan sivut tulee numeroida ja lukumäärä merkitä.
- Asiakirjoissa, jotka sisältävät metatietorakenteen, tulee turvallisuusluokka ilmaista lyhenteellä SAL.
- Käsiteltäessä tietoja sähköisesti tulee näytöissä näkyä kulloinkin käsiteltävän tiedon luokitus.
- Viranomainen, joka saa asiakirjan ulkomaiselta taholta, huolehtii, että asiakirjaan tulee kotimainen leima.

(Tietoaineistojen turvallinen käsittely 2008.)

Kuvio 3. Asiakirjojen leimat. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.4 Rekisteröinti

Rekisteröinnillä tarkoitetaan toimenpiteitä, joilla asiakirja merkitään diaariin tai vastaavaan rekisteriin, joka mahdollistaa viranomaisen tietovarannon seurantaa.

Diaaritieto (rekisteritieto) asianhallintajärjestelmissä sisältää tiedon asiakirjan suojaustasosta. Tämän avulla voidaan eri näkymillä tarjota eri suojaustasoihin kuuluvat asiakirjaluettelot. Tieto, joka tallennetaan diaarin julkiseen osaan, tulee olla julkista. Salassa pidettävien diaarien toteutuksessa tulee huomioida, että niitä pääsevät käsittelemään vain käyttöoikeuden omaavat.

- Asiakirjat tulee kirjata niitä varten määriteltyyn diaariin tai rekisteriin suojaustasojen mukaisesti.
- Diaarissa ja rekisterissä on suositeltavaa käyttää suojaustason lyhennettä ST II.

- Diaarissa ja rekisterissä on suositeltavaa käyttää turvallisuusluokituksen lyhennettä SAL (Tietoaineistojen turvallinen käsittely 2008.)

4.3.5 Kopiointi

Kopioinnilla tarkoitetaan toimenpiteitä, joilla alkuperäisestä asiakirjasta otetaan jäljennöksiä, kuten valokopio, tiedostojen kopiointi eri muistivälineille sekä asiakirjoista tai tietoaineistoista otetut otteet.

- Kopioita tulee käsitellä kuten alkuperäistä asiakirjaa.
- Sähköisten asiakirjakopioiden kohdalla tulee varmistaa asiakirjan eheys.
- Alkuperäisestä asiakirjasta saa ottaa sekä sähköisiä että paperimuotoisia kopioita, mutta kopiot on dokumentoitava ja jäljitettävyys varmistettava.
- Kopiot tulee leimata alkuperäistä asiakirjaa vastaavalla punaisella leimalla. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.6 Jakelu

Jakelulla tarkoitetaan toimenpiteitä, joilla päätetään salassa pidettävän tietoaineiston vastaanottajat, varmistetaan vastaanottajien tiedontarve, oikeus ja kyky käsitellä jaettavaa asiakirjaa.

- Asiakirjan allekirjoittaja määrää jakelun ja käsittelyprosessin.
- Asiakirjan tai sen osien jakelu tulee käydä ilmi asiakirjasta.
- Asiakirjan sisältämän tiedon perusteella jakelu määritellään niille, joita asiakirjan asiat koskettavat.
- Asiakirja tulee osoittaa henkilölle, määrättyä tehtävää hoitavalle tai organisaatiolle.
- Salassa pidettävän asiakirjan luovutus on dokumentoitava.
- Asiakirjan luovuttaminen edellyttää, että laissa on säädetty oikeus tiedon luovuttamiseen ja vastaanottajalla on oikeudet aineiston käsittelyyn ja kyky käsitellä sitä vaatimusten mukaan. Salassa pidettävän tiedon käsittely edellyttää, että henkilöstö tuntee käsittelysäännöt, omaa käsittelyoikeuden ja organisaatiolla on vaatimukset täyttävät tilat ja tietojärjestelmät. Salassa pidettävä tieto tulee luovuttaa jäljitettävästi sopimuksen mukaan.
- Kansainväliset asiakirjat jaellaan kansainvälisten sopimusten tai asiakirjan asettamien vaatimusten mukaisesti.
- Tietojärjestelmissä suoritetaan tietojen jakelu käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.7 Siirto

Siirrolla tarkoitetaan niitä toimenpiteitä, joilla asiakirjoista otetut kopiot siirretään jakelussa määrätyille henkilöille. Siirtoon voi käyttää esimerkiksi postia, sähköpostia tai myöntämällä käsittelyoikeudet.

- Salassa pidettävän asiakirjan jakelussa tulee varmistua siitä, etteivät asiattomat pääse salassa pidettävään tietoon käsiksi.
- Tietojärjestelmissä toteutetaan tietojen jakelu sähköpostin välityksellä tai tarjoamalla pääsyoikeus tietoon. Salassa pidettävän tiedon käsittely tulee tapahtua käyttöoikeuksien rajoitusten mukaan.
- Salassa pidettävää asiakirjaa luovutettaessa, lähettäjän on varmistettava, että vain henkilölle, jolla on tehtäviensä puolesta siihen oikeus, luovutetaan salattua tietoa.
- Käytettäessä sähköpostia siirtoon, on varmistuttava vastaanottajan osoitteesta.
- Salassa pidettävien tietoaineistojen ja tietojen siirto on sallittua vain sellaisissa tietojärjestelmien ja tietoverkkojen osissa, jotka täyttävät kyseisen suojaustason vaatimukset tietojen siirrolle.
- Manuaalinen asiakirjan siirto tapahtuu kuljetusyhtiön, kuten postin, välityksellä. Kansainvälisten asiakirjojen osalta noudatetaan myös osapuolten välisten sopimuksien määrittelemiä turvallisuusluokkakohtaisia menettelyjä. Kirjeet tulee aina toimittaa kirjattuna tai muulla vastaavalla tavalla läpinäkymättömään sinetöityyn sisäkuoreen sijoitettuna. Siirron edellytyksenä on lisäksi, että kuljetusyhtiön kanssa on olemassa ajantasainen sopimus turvallisuusjärjestelyistä. On myös suositeltavaa, että suojaustasoon II SALAINEN kuuluvat asiakirjat kuljetetaan kuriirin välityksellä.
- Salassa pidettävän tiedon käsittely puhelimessa ilman salauslaitetta on kiellettyä.
- Puhelimella, joka on varustettu viranomaisen hyväksymällä salauslaitteella(päästä päähän), voidaan salassa pidettäviä asioita käsitellä selväkielisenä.
- Salaamaton linjasiirto telefaxilla ei ole sallittu.
- Viranomaisen hyväksymällä salauslaitteella salattu linjasiirto telefax-laitteella on sallittu.
- Sähköisten asiakirjojen siirto avoimissa tietoverkoissa on sallittua vain salattuna. Jos käytetään sähköpostia, on varmistauduttava vastaanottajan osoitteesta.
- Sähköiset asiakirjat tulee siirtää salattuna myös korkean tietoturvatason verkoissa. Sähköisten asiakirjojen jakelussa on pidettävä erityistä huolta siitä, ettei sivullisten haltuun joudu asiakirjojen sisältämiä tietoja.
- Työasemien ja palvelimien kiintolevyjen, muistitikkujen ja muiden tallennusvälineiden sisältäessä salattua tietoa on muistivälineiden käsittelyssä noudatettava niiden sisältämän tiedon korkeinta suojaustasoa. Kiinteän työhuoneen ulkopuolella käytettävät muistivälineet tulee varustaa koko tietovarannon salaamilla menetelmillä. Lisäksi

kaikki tietojen siirto työvälineestä toiseen tulee kirjata ylläpidettävään lokiin kuten myös tiedon häviämiset. Tiedon taltiointi on sallittu vain erikseen valvottaviin muistivälineisiin. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.8 Vastaanottajan toimenpiteet

Vastaanottajan toimenpiteillä tarkoitetaan asioita, joita vastaanottajan pitää tehdä saadessaan salassa pidettävää tietoaineistoa käyttöönsä.

- Henkilön, joka vastaanottaa asiakirjan, on varmistuttava siitä, että lähettäjällä on oikeus kyseisen asiakirjan luovutukseen.
- Asiakirjan vastaanottajan tulee kirjata vastaanotettu aineisto diaariin tai rekisteriin.
- Vastaanottajan tulee kuitata tiedon vastaanotto.
- Vastaanottajan tulee kirjata vastaanotto.
- Vastaanottaja vastaa luovutuksen jälkeen kaikista asiakirjan käsittelyyn liittyvistä velvollisuuksista käsittely- ja käyttöoikeuksineen. Vastaanottajalla ei kuitenkaan ole oikeutta luovuttaa tietoa ulkopuolisille. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.9 Säilytys ja tallennus

Säilytyksellä ja tallennuksella tarkoitetaan toimenpiteitä, joita käytetään tiedon tallentamiseen tietojen valmistelu- ja käyttövaiheissa.

- Salassa pidettävä tieto tulee hallita koko elinkaaren ajan.
- Käyttäjän käsitellessä salassa pidettävää tietoa tulee hänen huolehtia vastuullaan olevasta tiedosta niin, ettei siihen pääse käsiksi muut kuin siihen käyttöoikeuden omaavat henkilöt.
- Tietovaranto, joka on suljetun verkon palvelimilla, tulee olla suojattuna käsittelyoikeuksilla. Lisäksi tiedon tulee olla salattuna.
- Käyttäjän on pidettävä huoli siitä, että tietojärjestelmä ei tallenna käsittelyn aikana syntyviä väliaikais- tai muita tallenteita ympäristöön, missä tietoon oikeudettomilla on pääsy tietoon.
- Työasemien ja palvelimien kiintolevyjen, muistitikkujen ja muiden tallennusvälineiden sisältäessä salattua tietoa on muistivälineiden käsittelyssä noudatettava niiden sisältämän tiedon korkeinta suojaustasoa. Kiinteän työhuoneen ulkopuolella käytettävät muistivälineet tulee varustaa koko tietovarannon salaamilla menetelmillä. Lisäksi kaikki tietojen siirto työvälineestä toiseen tulee kirjata ylläpidettävään lokiin kuten myös tiedon häviämiset. Tiedon taltiointi on sallittu vain erikseen valvottaviin muistivälineisiin.

- Käyttäjän on varmistettava, että asiakirjat joita hän käsittelee, tallentuvat niille tarkoitettuun ympäristöön. Organisaatioiden antamista ohjeista löytyy tarkempia tietoja.
- Säilytyksen ja tallennuksen osalta luonnosasiakirjoja käsitellään kuten vastaavia valmiita asiakirjoja.
- Salassa pidettävää tietoa sisältävät ulkoiset muistit tai vastaavat laitteet sekä paperimuotoiset asiakirjat tulee säilyttää niitä varten tarkoitetuissa turvakaapeissa, holveissa tai vastaavissa lukituissa ja valvotuissa tiloissa. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.10 Pääsy tietoon

Tietoon pääsyllä tarkoitetaan tilanteita ja menettelyitä, joilla käyttäjä saa salassa pidettävää tietoa käsittelyynsä. Tietojärjestelmissä toteutustapana ovat käyttövaltuushallinnan ja käyttäjän todentamisen keinot.

- Avoimeen tietoverkkoon liitetyssä työasemassa sähköisen asiakirjan lukeminen ja käsittely ei ole sallittua.
- Suljetun verkon palvelimilla olevan tietovarannon lukeminen on sallittua ainoastaan salattuna.
- Etäkäyttö ei ole sallittua. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.11 Arkistointi

Arkistoinnilla tarkoitetaan menettelyjä, joilla varmistetaan asetetun elinajan mukainen tiedon säilyminen. Arkistot on usein tapana sijoittaa käyttöympäristön ulkopuolelle.

- Arkistonmuodostussuunnitelmassa määritellään tietyt rakenteet ja vaatimukset mihin arkistoinnin tulee pohjautua.
- Käsittelyluokat ja sopimusten käsittelylle asettamat ehdot tulee ottaa huomioon arkistoinnissa.
- Kansainvälisten asiakirjojen arkistoinnissa tulee ottaa huomioon lainsäädäntö sekä sopimuksessa määritellyt tavat. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.12 Luokittelun päivittäminen ja poistaminen

Päivittämisellä tarkoitetaan asiakirjan salaamistarpeen arviointia. Arvioinnissa tulee huomioida, millaisia vaikutuksia salassapidolle on arviointihetkellä. Suojausvelvoite tulee poistaa, mikäli salassapidolle ei ole enää lainmukaisia perusteita.

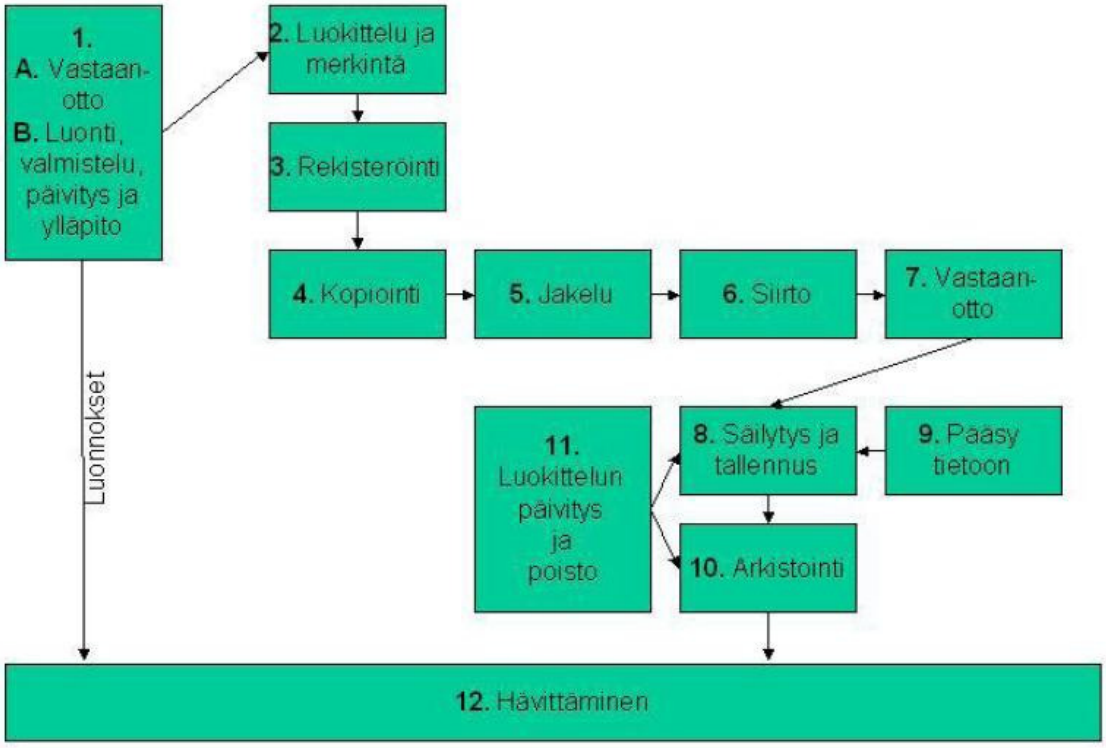
- Asiakirjan laatinut viranomainen suorittaa luokittelun uudelleenarvioinnin.
- Kun asiakirjan laadinnasta tai vastaanotosta on kulunut laissa mainittu suurin salassapitoaika, tulee asiakirja julkiseksi. Asiakirjaan tehdään merkintä, esimerkiksi salassapitomerkinnän yliviivaus. Asia tulee kuitenkin varmistaa asiakirjan laatineelta viranomaiselta.
- Jos asiakirjan suojaustasoa muutetaan arvioinnissa, tulee muutoksesta jäädä merkintä, allekirjoitus ja perustelu.
- Asiakirjan ja siitä otettujen kopioiden jakelussa mainituille tahoille tulee tiedottaa muutoksesta. (Tietoaineistojen turvallinen käsittely 2008.)

4.3.13 Tietoaineistojen hävittäminen

Tietoaineistojen hävittämisellä tarkoitetaan toimenpiteitä, joilla tarkoituksellisesti tuhotaan asiakirjoja tai muuta tietoaineistoa.

- Käyttötarpeen päätyttyä tulee alkuperäisasiakirjat hävittää arkistointisuunnitelman mukaisesti.
- Tarpeettomat asiakirjakopiot on hävitettävä välittömästi.
- Luonnosasiakirjat on hävitettävä välittömästi.
- Hävittämisen suorittamisessa pitää huolehtia siitä, että salassa pidettävät ja henkilötietoja sisältävät tiedot eivät joudu niihin oikeudettomien haltuun.
- Tiedon tuottaja on vastuussa valmisteluvaiheessa ja organisaation käyttöön luovuttamattoman tietovarannon hävittämisestä
- Organisaation valtuuttama henkilö on vastuussa valmiiden, viranomaisen asianhallintajärjestelmän sisältämien asiakirjojen hävittämisestä.
- Suojaustasoon II kuuluvat asiakirjat hävittää valtuutettu organisaation määräämä vastuuhenkilö. Asiakirjoihin tutustuneista taltioidaan hävittämisen yhteydessä luettelo. Sähköisissä järjestelmissä tallennetaan käsittelytiedon sisältävät lokitiedostot tai vastaavat.
- Alkuperäisen asiakirjan hävittämisestä vastaa arkistonhoitaja. Esimerkiksi määräaikaisesti säilytettävien asiakirjojen tai sähköisten asiakirjojen kohdalla asiakirjat eivät välttämättä siirry arkistonhoitajalle ja näissä tapauksissa asiakirjan haltija on vastuussa käsittelyluokan edellyttämän tavan mukaisesta hävittämisestä.

- Sähköisten tiedostojen tuhoaminen työasemilta, palvelimilta sekä muilta muistivälineiltä tulee suorittaa viranomaisen antamien tarkempien ohjeiden mukaan. Ja tulee myös ottaa huomioon, ettei normaali delete-napin painaminen ole riittävää.
- Tietojärjestelmiä käytettäessä syntyvät väliaikaistiedostot on poistettava riittävän usein.
- Kaikki muistivälineet, jotka sisältävät salattua tietoa, tulee hävittää viranomaisten antamien ohjeiden mukaisesti.
- Tietojärjestelmissä sekä tietovarannoissa olevan tiedon hävittämisessä tulee käyttää tietovarannolle määriteltyjä vaatimuksia.
- Paperimuotoiset asiakirjat tulee hävittää joko valvotusti polttamalla tai silppuamalla tarpeeksi pieneksi. (Tietoaineistojen turvallinen käsittely 2008.)



Kuva 4. Tietoaineiston elinkaari. (Tietoaineistojen turvallinen käsittely. 2008.)

5 Verkon rakentaminen

Tässä luvussa käsitellään niitä vaatimuksia, joita turvallisuusluokka II:n mukaisen materiaalin käsittely edellyttää tilalta sekä tilassa olevalta tietoverkolta, jossa materiaalia käsitellään. Lisäksi luvussa käsitellään keinoja sekä vaihtoehtoja, joilla kyseiset vaatimukset saadaan täytettyä. Salassa pidettävän tiedon käsittely edellyttää, että henkilöstö tuntee käsittelysäännöt, omaa käsittelyoikeuden ja organisaatiolla on vaatimukset täyttävät tilat ja tietojärjestelmät.

5.1 Tila

Kuten edellisessä luvussa oli tarkasti eritelty, tarvitsee salassa pidettävän (turvallisuusluokka II) aineiston käsittelyssä noudattaa tarkkoja sääntöjä sekä pitää huoli siitä, etteivät tietoon pääse käsiksi kuin sellaiset henkilöt, joilla on oikeus ja tarve kyseisen tiedon käsittelyyn. Myös tietojärjestelmiin, joissa liikkuu tai säilytetään suojattua materiaalia, tulee pääsyn olla valvottua, sekä luvaton tunkeutuminen tulee estää käytettävissä olevin keinoin.

Asiakirjojen tietojenkäsittely- ja säilytystilat tulee olla riittävän valvottuja ja suojattuja. Tilaan tulisikin olla asiattomilta pääsy estetty ja samaan aikaan sallittujen henkilöiden tulisi päästä kulkemaan tilassa mahdollisimman vapaasti. Olisi myös hyvä, että voidaan reaaliaikaisesti sekä jälkeenpäin seurata keitä on tilassa milläkin hetkellä ollut. Kulunvalvonta on hyvä ja erittäin tärkeä keino, jolla voidaan rajoittaa ja seurata sitä, kuka pääsee tilaan, jossa on salattua materiaalia.

Kulunvalvontajärjestelmän avulla saadaan arkaluontoinen tieto suojattua, oikeutettujen henkilöiden hallittu kulku hoidettua ja asiattomien henkilöiden liikkuminen halutuissa tiloissa estettyä. Tämä tapahtuu ohjaamalla ovien sähkölukkoja kulunvalvontalukijoilla, joita taas hallitaan kulunvalvontaohjelman avulla päätietokoneelta. Ohjelmaan on mahdollista syöttää ovikohtaiset tiedot sallituista henkilöistä sekä ryhmistä myös ajan tai rakennusten perusteella. (Työajanseurannan yhdistäminen kulunvalvontaan 2005.)

Kulkutapahtumia on mahdollista tarkastella reaaliajassa tai raporttien muodossa eri kriteerien pohjalta, kuten esimerkiksi ajankohdan, oven tai henkilön. Järjestelmästä voidaan myös tarkastella, ketkä ovat olleet tiettyyn aikaan tilassa. (Työajanseurannan yhdistäminen kulunvalvontaan 2005). Tällaisessa tilassa on erittäin tärkeää, että on mahdollista valvoa ketä tilassa vierailee ja että asia on myös jälkeenpäin mahdollista selvittää, jos tulee tarve.

Turvallisuusluokka II ei salli avoimeen tietoverkkoon liitetyssä työasemassa salattujen asiakirjojen lukemista ja käsittelyä, ja edellyttääkin, että verkko on eristetty kaikista muista verkoista täysin. Kaapelointi tuleekin suorittaa siten, ettei tilan ulkopuolelta ole mahdollisuutta yhdistyä verkkoon. Langattoman lähiverkon käyttöönottoon turvalaboratoriossa tuskin on tarvetta, mutta se ei myöskään ole suositeltua, koska langattoman lähiverkon kuuluvuusalue ulottuu tilan ulkopuolelle. Jos langaton lähiverkko on suoraan kytketty sisäverkkoon, on olemassa riski, että langattoman lähiverkon kautta voidaan tunkeutua sisäverkon järjestelmiin, vaikka kaikki käytettävissä olevat suojaus- ja salauskeinot olisivatkin käytössä. (Langattomien lähiverkkojen (WLAN) turvallisuus 2008).

Asiakirjoja saattaa olla useassa eri muodossa. Tallennus- ja esitysmuodosta huolimatta tulee asiakirjojen käsittelyssä noudattaa luokituksen käsittelyvaatimuksia. Tätä varten tilassa tulee myös olla turvakaappi, holvi tai vastaava lukittu ja valvottu tila, missä voidaan säilyttää salassa pidettävää tietoa sisältävät ulkoiset muistit tai vastaavat laitteet, sekä paperimuotoiset asiakirjat. Tilassa tulee olla myös turvallinen laitetila minne voidaan sijoittaa palvelimet sekä verkon aktiivilaitteet.

5.2 Verkon tiedostopalvelin

Tiedostojen jakopalvelu on ehdottomasti lähiverkkojen käytetyin palvelu.(Hakala, M., Vainio, M. 2005). Verkoissa, joissa on useampi työasema, on kannattavaa keskittää sähköisten dokumenttien sekä muiden tiedostojen säilytys. Tähän tarkoitukseen tiedostopalvelin on hyvä ratkaisu, koska sinne voidaan keskitetysti ja järjestelmällisesti tallentaa suuria määriä tietoja. Keskitetty tiedonsäilytys tehostaa tiedon hallintaa ja käsittelyä sekä nopeuttaa huomattavasti tiedon hakemista. Kaikki työasemat voivat tallentaa palvelimelle tiedostoja, ja tiedot ovat kaikkien työasemien käytettävissä.

Verkoissa, joissa käsitellään turvaluokiteltua materiaalia, käsitellään myös tietoa joka ei vaadi turvaluokittelua. Luokittelemattoman tiedon tallentamiseen ja jakamiseen keskitetty palvelinratkaisu onkin hyvä, mutta turvaluokiteltu materiaali ei kuitenkaan saa olla kaikkien käytettävissä, joten sitä varten tulee palvelimella ottaa käyttöön tiettyjä ratkaisuja.

Turvallisuusluokka II:n mukaan luokiteltu tietovaranto, joka sijaitsee suljetun verkon palvelimella, tulee olla suojattuna käsittelyoikeuksilla. Käyttöoikeudet tulee myös rajata asianmukaisesti ja käyttöä pitää valvoa riittävästi. Palvelimella oleva tieto pitää myös olla salattuna.

Lähiverkkojen käyttäjähallinnassa on kaksi perusratkaisua, joista vanhempi eli vertaisverkko on nykyään harvemmin käytettävissä. Vertaisverkoissa järjestelmät jakavat keskenään resursseja, ilman keskitettyä yhteistä järjestelmää. Nykyään suurin osa käytössä olevista lähiverkkojärjestelmistä perustuu keskitettyihin eli dedikoituihin järjestelmiin, jotka voidaan jakaa kahteen osaan: jaettuihin käyttäjäkantoihin ja hakemistopalveluihin. (Hakala ym. 2005, 30.)

Dedikoiduissa verkoissa lähiverkon työasemat ja palvelimet hyödyntävät keskitettyä käyttäjäkantaa, joka yksinkertaistaa hallintamallia ja helpottaa järjestelmän ylläpitoa. Jaetun käyttäjäkannan järjestelmien verkossa on yksi tai useampi hallintapalvelin, joka ylläpitää keskitettyä käyttäjäkantaa. Käyttäjän kirjautuessa verkkoon hänen tietonsa tarkastetaan hallintapalvelimelta. (Hakala ym. 2005, 32.)

Toimialuejärjestelmässä toimialueen pääpalvelin, primary domain controller, vastaa toimialueen käyttäjäkannasta. Järjestelmästä löytyy lisäksi yksi tai useampia varahallintapalvelimia, eli backup domain controlleria. Käyttäjäkannan hallintaoperaatiot suoritetaan pääpalvelimella, joka on järjestelmän ainoa palvelin jossa käyttäjäkantaa pystyy muuttamaan. Nämä muutokset päivitetään varahallintapalvelimiin, mikä varmistaa ajantasaisen käyttäjäkannan löytymisen useammalta kuin yhdeltä palvelimelta. (King, R. 2003, 75-76.)

Suojattua tietoa sisältävät asiakirjat tulee rekisteröidä tai niitä tulee muulla tavoin hallita. Henkilöistä, jotka tutustuvat turvallisuusluokka II:n mukaan luokiteltuihin asiakirjoihin, tulee jäädä täydellinen kopiokohtainen jälki, jotta on mahdollista seurata asiakirjoista otettuja kopioita suojaustarvetta edellyttävältä ajalta. Salassa pidettävän asiakirjan luovutus on dokumentoitava.

Salassa pidettävää sähköistä asiakirjaa käsitellessä tulee tapahtuman kirjautua automaattisesti sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai itse asiakirjaan. Suositeltavin vaihtoehto näistä on loki tai vastaava sähköinen apuväline.

Loki on tietynlainen tapahtumarekisteri, joka yleensä automaattisesti kerää erilaista tietoa järjestelmän toiminnasta ja toimimattomuudesta. Yleensä lokitieto tallentuu erilliseen lokitiedostoon, joka saattaa olla yksinkertainen tekstitiedosto. Lokiin tallentuva tieto on yleensä tärkeää erityisesti jälkikäteen tapahtuvien ongelmatilanteiden selvittelyssä.

Verkossa, jossa käsitellään turvallisuusluokka II:n mukaan suojattua tietoa, tulisi olla järjestelmä, joka tallentaa lokiin automaattisesti tietoa suojatun materiaalin käsittelystä. Lokiin tulisi automaattisesti tallentua asiakirjan käsittelystä olennaisia tietoja, kuten kuka on käsitellyt asiakirjaa ja milloin asiakirjaa on käsitelty.

Lisäksi tulisi järjestelmässä olla rekisteri tai loki, jonne tallennetaan tietoja, kuten asiakirjojen vastaanotto, asiakirjan luovuttaminen, asiakirjoista otetut kopiot, tietojen siirto, tietojen häviämiset jne.

5.3 Tiedon hävittäminen

Kun tietokoneesta poistetaan tiedosto laittamalla se roskakoriin ja tyhjentämällä roskakori, tiedosto ei oikeasti ole vielä poistunut minnekään. Tämän toiminnan jälkeen tiedosto on vielä samassa paikassa kuin aiemminkin. Ainoastaan tiedostojärjestelmään on merkitty, että kohta, missä tiedosto sijaitsi, on tyhjä ja siihen voi kirjoittaa päälle. Ennen kuin tiedoston päälle todella kirjoitetaan mitään, on tällainen tiedosto helposti palautettavissa siihen tarkoitetuilla

ohjelmilla. Jos tiedosto halutaan poistaa lopullisesti, on sen päälle kirjoitettava tietoa, mielellään useampaan kertaan.

Tiedon turvalliseen hävittämiseen löytyy runsaasti eri ohjelmia eri käyttöjärjestelmille sekä maksullisena että ilmaisena. Blancco File Shredder on yksi esimerkki maksullisesta tiedostonhävitysohjelmasta Windows-koneelle. Ohjelmassa saa valita, kuinka monta kertaa halutaan kirjoittaa tuhottavan tiedoston päälle. (Blancco File Shredder 2009). Myös ilmaisella Eraser-ohjelmalla onnistuu tiedostojen turvallinen poistaminen päällekirjoittaen Windows-koneissa. (Eraser 2009). Myös Unix- ja Linux-järjestelmiin löytyy useita ohjelmistoja, joilla onnistuu tiedoston turvallinen poistaminen. Esimerkiksi shread-, srm- ja sfill- komennot ovat yksinkertaisia ohjelmia tiedostojen poistoon. Shread-komento kuuluu useaan Linux-jakeluun valmiiksi, mutta sen saa helposti asennettua pakettienhallinnan kautta, jos se puuttuu. Srm- ja sfill-paketit tulee yleensä asentaa erikseen, ja ne tulevat secure delete-paketin mukana. Shred-komennolla voi kirjoittaa tiedostojen, osioiden ja massamuistien päälle. Srm-komentoa käytetään tiedostojen ylikirjoittamiseen ja sfill-komentoa käytetään tyhjän levytilan ylikirjoittamiseen(Howto Delete Files Permanently and Securely in Linux 2009.)

Kun sähköisiä tiedostoja tuhotaan työasemilta, palvelimilta sekä muilta muistivälineiltä kuten muistitikuilta ja muistikorteilta, tulee tiedostot tuhota turvallisesti. Suojaustasoon II kuuluvien asiakirjojen asianmukaiseen tuhoamiseen tulisi organisaation määrätä vastuuhenkilö, joka pitää huolen siitä, että tiedostot tuhotaan luokittelun mukaisten vaatimusten mukaan. Asiakirjaa hävitettäessä tulee taltioida luettelo asiakirjaan tutustuneista henkilöistä. Sähköisissä järjestelmissä taas tallennetaan lokitiedot tai vastaavat, jotka sisältävät tiedot tietojen käsittelystä.

Tietoja käsitellessä syntyy automaattisesti väliaikaistiedostoja, joiden poistamisesta tulee huolehtia riittävän usein. Hävittämisen yhteydessä tulee pitää huoli, ettei salassa pidettäviä ja henkilötietoja sisältäviä tietoja joudu niihin oikeudettomien haltuun.

Väliaikaistiedostojen poistaminen voidaan hoitaa esimerkiksi ohjeistamalla käyttäjät tyhjentämään itse väliaikaistiedostot. Väliaikaistiedostojen poisto käsin on työlästä, joten siihenkin on tehty useita ilmaisia ja maksullisia ohjelmia. Ccleaner on Windows-koneille tarkoitettu hyvä ilmainen ohjelma, jolla voidaan poistaa väliaikaistiedostot päällekirjoittaen tai ilman. Ohjelmalla voidaan puhdistaa myös Windowsin rekisteri. (Ccleaner 2009). Linux-käyttöjärjestelmä tallentaa väliaikaistiedostot /tmp-kansioon ja väliaikaistiedostot tyhjennetään automaattisesti uudelleenkäynnistyksen yhteydessä. Linuxiin on myös puhdistusohjelmia, joilla saadaan edistyneempää väliaikaistiedostojen puhdistusta. Aiemmin mainittua sfill-komentoa voidaan käyttää esimerkiksi /tmp-hakemiston tyhjän tilan ylikirjoittamiseen, jos halutaan ylikirjoittaa poistetut tiedostot.

Väliaikaistiedostojen poistamisen voi myös hoitaa siihen tarkoitetulla skriptillä, eli komentosarjalla esimerkiksi kirjauduttaessa ulos työasemalta. Skriptikielillä kirjoitettavilla skripteillä voidaan automatisoida tietokonejärjestelmissä useita tehtäviä ilman varsinaista ohjelmointikieltä. Yleisimpiä skriptikieliä Linux/Unix-käyttöjärjestelmissä ovat sh ja bash, sekä Windows-käyttöjärjestelmissä bat-tiedostot.

5.4 Käyttäjien kouluttaminen

Henkilöille, joille annetaan oikeudet salattuun tietoon sekä pääsy tilaan missä tietoa käsitellään, tulee myös tuoda ilmi kaikki vaatimukset, joita heitä kohtaan on sekä säännöt joita tulee noudattaa. Käyttäjän on pidettävä huoli, että käsitellessään salattua tietoa tietoon ei pääse käsiksi kukaan kenellä ei ole oikeutta tietoon. Tässä tulee olla erityisen tarkka silloin, kun samassa tilassa on henkilöitä, joilla ei ole oikeutta salattuun tietoon.

Työtilasta poistuttaessa asiakirjoja ei saa jättää ilman valvontaa. Tämä tarkoittaa käytännössä sitä, että kun työtilasta poistutaan, tulee työasemat lukita sekä mahdolliset paperiset asiakirjat laittaa kassakaappiin tai vastaavaan lukittuun tilaan.

Tietojärjestelmien kohdalla käyttäjän on pidettävä huoli siitä, että tietojärjestelmä ei tallenna käsittelyn aikana syntyviä väliaikais- tai muita tallenteita ympäristöön, missä tietoon oikeudettomilla olisi mahdollisuus päästä tietoon käsiksi. Käyttäjän on myös oltava tarkkana, että tallennettaessa tietoja ne tallentuvat oikeaan paikkaan. Tietojärjestelmät, jotka tuottavat automaattisesti esimerkiksi valvonta-, loki- tai muuta salassa pidettävää tietoa, velvoittavat käsittelijää varmistamaan oman oikeutensa salattuun tietoon.

Käyttäjän tulee myös pitää huolta aineistoa valmisteltaessa, että aineistoa tulee koko prosessin ajan käsitellä ympäristössä, jossa vain käyttöoikeuden omaavat pääsevät aineistoon käsiksi.

5.5 Tiedonsiirto ja jakelu

Tilassa tuotettua salattua tietoa tarvitsee siirtää ja jakaa sekä verkon sisä- että ulkopuolella. Verkon sisällä tiedon jakaminen on helppoa, sillä järjestelmässä tarvitsee vain sallia halutuille henkilöille pääsyoikeudet tietoon. Turvallisuusluokitellun tiedon jakaminen tilan ulkopuolelle sisältää omat riskinsä ja siitä syystä onkin asioita mitä pitää ottaa huomioon tiedon jakamisessa.

Sähköisten asiakirjojen jakelussa on pidettävä erityistä huolta siitä, ettei sivullisten haltuun joudu asiakirjojen sisältämiä tietoja. Sekä suljetuissa tietojärjestelmissä että avoimissa tietojärjestelmissä tapahtuvan turvaluokitellun tiedon siirto tulee aina olla salattua. Kuitenkin tulee ottaa huomioon, että tiedonsiirto on sallittua vain sellaisissa tietojärjestelmien ja tietoverkkojen osissa, jotka täyttävät kyseisen suojaustason vaatimukset tietojen siirrolle. Jos tiedon siirtoon käytetään sähköpostia, tulee varmistua vastaanottajan osoitteesta. On myös varmistuttava siitä, että vain henkilölle, jolla on tehtäviensä puolesta siihen oikeus, luovutetaan salattua tietoa.

Käsiteltäessä salassa pidettävää tietoa puhelimessa, tulee käyttää viranomaisen hyväksymää salauslaitetta. Myös linjasiirto telefaxilla vaatii viranomaisen hyväksymän salauslaitteen. Asiakirjan siirto manuaalisesti tulee tapahtua Itellan tai vastaavan kuljetusyhtiön välityksellä. Siirron edellytyksenä on ajantasainen sopimus kuljetusyhtiön kanssa turvallisuusjärjestelyistä. Kirjeet tulee aina toimittaa kirjattuna tai vastaavalla tavalla läpinäkymättömään sinetöityyn sisäkuoreen sijoitettuna. On myös suositeltavaa, että asiakirjat kuljetetaan kuriirin välityksellä.

6 Tiedostopalvelimen toteuttaminen turvallisessa tilassa

Tiedostopalvelin voidaan asentaa monelle eri alustalle. Yleisimpiä alustoja, joiden päälle tiedostopalvelin voidaan asentaa, ovat Unix, Linux ja Windows. Unix ja Windows ovat kaupallisia, suljettuun lähdekoodiin perustuvia käyttöjärjestelmiä, kun taas Linux on ilmainen, avoimeen lähdekoodiin perustuva käyttöjärjestelmä.

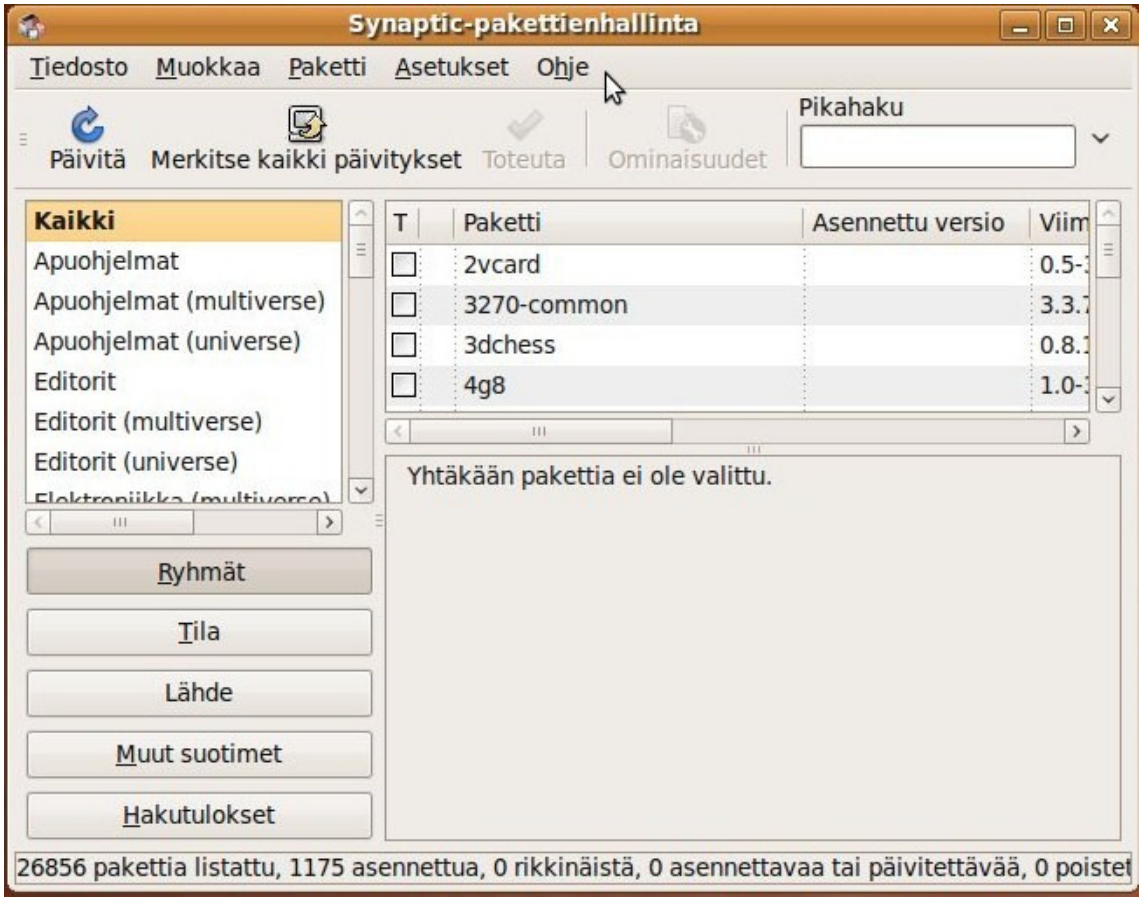
Turvallisuus, käyttövarmuus, vakaus ja hinta ovat palvelinkäytössä tärkeimpiä ominaisuuksia. Turvalabran tapauksessa turvallisuuden tärkeys korostuu, koska kyseessä on turvallinen ympäristö. Linuxissa on juuri tietoturvan osalta useita etuja muihin mahdollisiin järjestelmiin nähden. Lähdekoodin avoimuus on yksi suurimmista. Kuka tahansa voi tarkastaa Linuxin ohjelmakoodin mahdollisten tietoturvariskien, aukkojen ja ohjelmointivirheiden varalta, sekä tarvittaessa muokata järjestelmää omanlaisekseen. Mahdollisiin turva-aukkoihin saadaan Internetistä vapaaehtoisten ohjelmoijien tekemiä paikkauksia nopeasti, toisin kuin kaupallisen yrityksen hallitsemissa suljetun lähdekoodin järjestelmissä. Linuxissa on myös Unixista peritty ominaisuus, ettei järjestelmää ajeta pääkäyttäjän täysin oikeuksin kuin tarvittaessa. Kun käyttäjällä on kirjoitusoikeudet vain omiin tiedostoihinsa, mahdolliset haittaohjelmatkaan eivät pääse leviämään käyttäjän tiedostoja pitemmälle.

Tässä luvussa käsitellään Linuxia yleisesti, sekä selvitetään, minkälaisia eri vaihtoehtoja Linux tarjoaa, tiedostopalvelimen, joka kerää lokitietoja, toteuttamiseksi. Lisäksi selvitetään turvalabran näkökulmasta eri tekniikoiden ja ohjelmien hyviä ja huonoja puolia, joita kannattaa ottaa huomioon labran suunnittelussa.

Linux

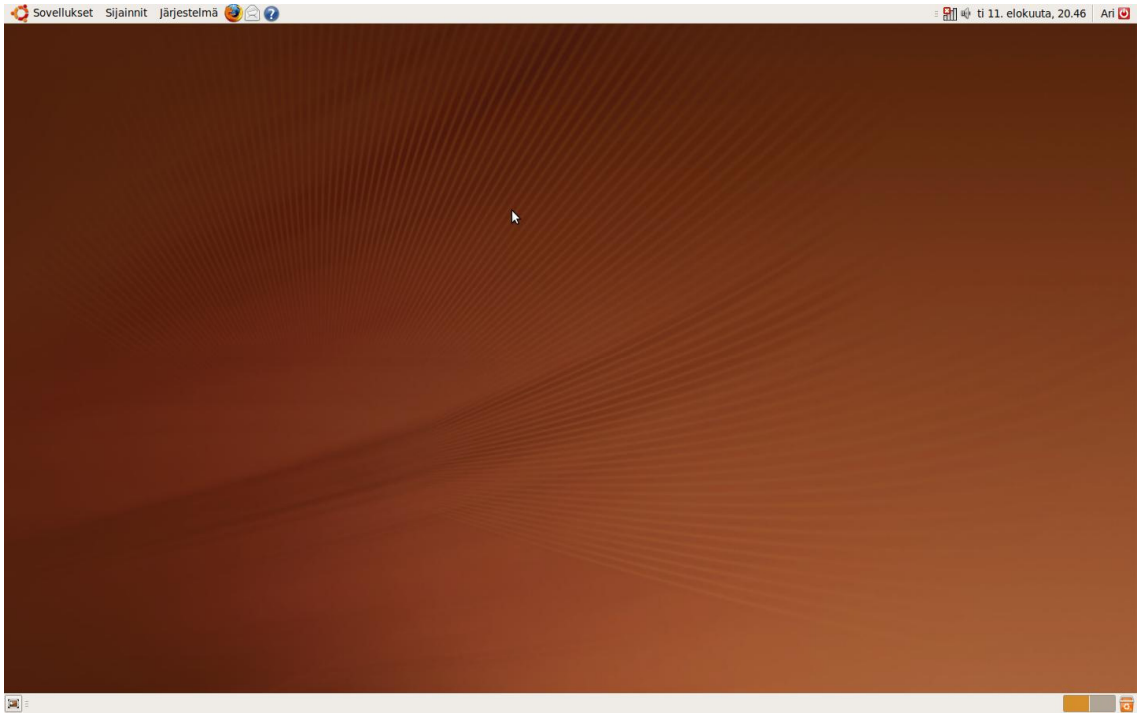
Linux on Unix-sukuinen vapaa käyttöjärjestelmä. Virallisesti Linux tarkoittaa pelkkää käyttöjärjestelmän ydintä (engl. kernel), joka on käyttöjärjestelmän keskeisin osa ja joka mahdollistaa muiden ohjelmistojen toiminnan. (Barkakati, N. 2006, 10). Linuxin ytimen loi alun perin suomalainen Linus Torvalds opiskellessaan Helsingin yliopistossa vuonna 1991. Linux perustuu avoimeen lähdekoodiin, tarkemmin GNU GPL- lisenssiin. Avoimen lähdekoodin ohjelmissa lähdekoodi on kaikkien nähtävillä, ja kaikilla on lupa käyttää, muuttaa ja levittää avoimen lähdekoodin ohjelmia, muutettuna tai muuttamattomana maksutta tai maksua vastaan, kunhan vain lähdekoodi pysyy avoimena. Edellä mainitun avoimuuden johdosta kuka tahansa voi valmistaa oman käyttöjärjestelmän Linux-ytimen ympärille, kuten useat organisaatiot ja yritykset tekevätkin.(Kuutti, W., Rantala, A. 2007.)

Vaikkakin Linux virallisesti tarkoittaa pelkkää käyttöjärjestelmän ydintä, yleensä Linuxista puhuttaessa tarkoitetaan kokonaista käyttöjärjestelmää, eli jotakin jakelupakettia. Jakelupaketista käytetään myös nimeä distro, joka tulee englanninkielisestä sanasta distribution. Jakelupaketti koostuu Linux-ytimestä ja sen ympärille kootusta ohjelmistokokonaisuudesta. Kaikkiin jakelupaketteihin kuuluu ytimen ja vapaiden ohjelmistojen lisäksi jakelun asennusohjelma ja ohjelmapakettien hallintasysteemi sekä joissain tapauksissa jakeluun saattaa kuulua myös kaupallisia ohjelmia. (Kuutti ym. 2007, 9). Linuxin vapaudesta johtuen eri jakelujen käyttäjämääriä, sekä markkinaosuuksia on mahdotonta arvioida tarkasti. Maailmanlaajuisesti suosituimpia Linux-jakeluita ovat: Debian GNU/Linux, Ubuntu, Fedora, Gentoo, SUSE, Mandriva ja Red Hat. (Kuutti ym. 2007, 10). Yhteisestä ytimestä huolimatta saattavat eri Linux jakelut erota toisistaan hyvinkin paljon. Eri jakelut saattavat soveltua eri tarkoituksiin, mutta usein käyttäjän oma mielipide ratkaisee mikä jakeluista on paras. Mitä suositumpi jakelu on kyseessä, sitä helpompaa on löytää apua mahdollisiin ongelmatilanteisiin. Esimerkiksi Usenet News uutisryhmistä löytyy runsaasti apua. (Barkakati, N. 2006, 235–236) Eri jakeluita voidaan jakaa luokkiin niiden käyttämän paketinhallintajärjestelmän mukaan. Muun muassa Debian ja Ubuntu käyttävät .deb paketteja käyttävää dpkg/apt paketinhallintajärjestelmää. Red Hat Linuxin aloittamaa .rpm paketteja käyttävää järjestelmää käyttävät mm. Fedora, Mandriva ja SUSE. Muista järjestelmistä poiketen Gentoo ei käytä binääripaketteja ollenkaan, vaan paketit sisältävät ohjelmien lähdekoodin, joka käännetään ohjelmaa asennettaessa. (Kuutti ym. 2007, 11–12.)



Kuva 5. Ubuntun graafinen synaptic pakettienhallinta ohjelma.

Linuxin eri jakelupaketeille on saatavilla useita eri työpöytäympäristöjä, jotka tarjoavat graafisen käyttöliittymän käyttöjärjestelmälle. Linuxin palvelinversioissa ei yleensä tule oletuksena graafista käyttöliittymää mukana, mutta sen saa tarvittaessa helposti asennettua, jos pelkkä komentorivin käyttö ei jostain syystä riitä. Suosituimpia työpöytäympäristöjä ovat KDE, Gnome ja Xfce. Linux jakeluissa on yleensä valmiina jokin tietty työpöytäympäristö, mutta sen voi tarvittaessa vaihtaa helposti pakettienhallinnan kautta.



Kuva 6. Ubuntu Linuxin Gnome työpötä

Linuxissa on useita vahvuuksia, jotka tekevät siitä varteenotettavan kilpailijan muille järjestelmille. Linuxia pidetään erittäin vakaana käyttöjärjestelmänä, eikä sitä tarvitse koko ajan käynnistellä uudelleen. Linux on myös edullisempi, koska siitä ei tarvitse maksaa kalliita lisenssejä, vaan sen voi kuka vaan kopioida ilmaiseksi verkosta. Myös yhteensopivuus on Linuxin vahvuuksia, sillä se toimii hyvin monella erityyppisellä tietokoneella ja sitä voi tarvittaessa muokata omaan käyttöön sopivaksi. Unix-sukuisuus tulee Linuxissa hyvin esiin hyvinä verkko-ominaisuuksina ja erityisesti TCP/IP-pohjaiset internetiin tarjottavat palvelut ovat huomattava vahvuus. Myös tietoturvaa, avoimen lähdekoodin tuomaa avoimuutta sekä Linux-yhteisön vahvaa tukea järjestelmään liittyvissä ongelmissa voidaan pitää Linuxin vahvuutena. (Kuutti ym. 2007, 27–30.)

Linuxin heikkouksina voidaan pitää sitä, että Linux-järjestelmät eroavat jonkin verran toisistaan esimerkiksi eri jakeluiden sekä eri työpöytien toiminnan osalta, jolloin saattaa tulla ongelmia, kun asiat eivät toimikaan totutulla tavalla. Myös eri järjestelmien ohjelmien yhteensopimattomuutta voidaan pitää suurena ongelmana, vaikkakin Linuxille on olemassa erilaisia emulaattoreita, jolla esimerkiksi joitain Windows-ohjelmia voidaan ajaa Linux järjestelmällä. (Kuutti ym. 2007, 31.)

Linuxia käytetään tällä hetkellä eniten monenlaisissa palvelintehtävissä sekä erilaisissa sulautetuissa järjestelmissä. Linuxin vahvuutena ovat TCP/IP-pohjaiset Internetiin tarjottavat palvelut. Linuxia pidetään yleisesti myös vakaampana kuin Windowsia. (Kuutti ym. 2007, 2-3.) Linuxia käytetään myös useissa ympäristöissä, joissa turvallisuuden osalta on normaalia suu-

rempia vaatimuksia, kuten esimerkiksi pankeissa ja finanssilaitoksissa. Esimerkiksi Wall Streetillä usean rahoitusyhtiön tietojärjestelmät ovat Linux-pohjaisia. (Linux valtaa Wall Streetiä. 2008). Myös suuret pankit useissa eri maissa luottavat Linuxiin, kuten Kiinassa (Chinas's largest bank switches to Linux. 2005), sekä Brasiliassa. (Avoin ohjelmakoodi valtaa pankkeja Brasiliassa. 2004).

Todellisia markkinaosuuksia ja käyttäjämääriä on Linuxin vapaasta jakelusta johtuen mahdotonta tietää, mutta erilaisia arvioita voidaan esittää. Tutkimusyhtiö IDC:n mukaan palvelimissa Linuxin osuus vuoden 2006 lopussa oli noin 46 prosenttia, Microsoftin osuus 24 prosenttia sekä muiden järjestelmien loput 30 prosenttia. (Kuutti ym. 2007, 32). Linux alkaa yleistyä myös työasemakäyttöjärjestelmänä, mutta prosentuaalisesti sen osuus on edelleen lähes olematon. Vuonna 2009 www-sivujen käyttötilastoon perustuvassa tutkimuksessa Linux ylitti ensimmäistä kertaa yhden prosentin rajan. (MikroBitti. 6/2009, 11).

6.1 Tiedostopalvelin Linuxilla

Tiedostopalvelimella tarkoitetaan palvelimella sijaitsevan kansion tai kansioiden jakamista verkon muiden koneiden kesken siten, että verkon muilta koneilta voidaan käyttää kansiota ja siellä sijaitsevia tiedostoja aivan kuin ne olisivat omalla koneella. Tiedostopalvelimen toteuttaminen Linuxilla on helppoa ja kustannustehokasta, sillä kuka vain voi ladata Linuxin eri jakeluita internetistä ilmaiseksi ilman kalliita lisenssimaksuja. Lisäksi Linuxiin on paketinhallintajärjestelmän kautta saatavana runsas valikoima ilmaisia ohjelmia, joilla on mahdollista toteuttaa lähes mitä vain. Myös Linuxin ja ohjelmien käyttöön, sekä mahdollisiin ongelmatilanteisiin löytyy runsaasti apua kirjojen, uutisryhmien, Linuxiin keskittyvien sivustojen, jakelujen kotisivujen, IRC-kanavien, keskustelupalstojen sekä ohjelmien sisäisten ohjetiedostojen kautta.

Linux jakelua valitessa ei ole yhtä oikeaa vaihtoehtoa mikä distro kannattaa valita. Huomioon otettavia asioita ovat esimerkiksi: mihin tarkoitukseen palvelin tulee, onko johonkin tiettyyn jakeluun jo valmiiksi tuntemusta/mieltymystä, soveltuuko jokin jakelu paremmin palvelin tarkoitukseen vakauden tai muun syyn takia, kuinka aktiivista on palvelimen ylläpito tai tuleeko käyttöön jotain tarpeellisia ohjelmistoja jotka toimivat vain jossain/joissain tietyissä jakeluissa. Usein eri jakeluilla on palvelinkäyttöön ja työasemakäyttöön omat asennusversiot, jolloin palvelinversiosta usein puuttuu graafinen käyttöliittymä, sekä niissä on mahdollista asentaa tarpeelliset palvelinohjelmistot jo käyttöjärjestelmän asennusvaiheessa. Palvelinkäyttöön tulevan jakelun on myös hyvä olla sellainen, että jakelun versiota tuetaan riittävän pitkään päivitysten osalta ilman, että koko järjestelmää tarvitsee jatkuvasti päivittää uuteen versioon.

Linux-palvelimeen, josta halutaan jakaa tiedostoja, pitää asentaa palvelinohjelmisto, jolla tiedostojen jako muille koneille hoidetaan. Kaksi yleisintä tiedostojenjako-ohjelmaa ovat Samba sekä NFS (Network File System). NFS on asiakas/palvelin-periaatteella toimiva alun perin Sun Microsystemsin kehittämä käytäntö, jonka avulla tiedostoja voidaan jakaa verkon kautta. (NFS. 2009). NFS on tarkoitettu Unix-sukuisten käyttöjärjestelmien väliseen tiedostojen jakoon, mutta toimii myös muilla käyttöjärjestelmillä, jos niihin on asennettu NFS asiakasohjelma. (Barkati, N. 2006, 661). Samba on Windowsissakin käytettyyn SMB/CIFS-tiedostonsiirtoprotokollaan pohjautuva avoimen lähdekoodin ohjelma, jonka avulla Linux-koneella sijaitsevia kansioita voidaan jakaa helposti samassa verkossa oleville muille koneille. (What is samba. 2009). Jos verkossa on Windows-koneita, on Samban käyttö kannattavampaa kuin NFS:n, koska Samba toimii Windows-koneiden kanssa ilman ylimääräisiä asiakasohjelmia. Samban avulla Linux-koneesta voidaan myös tehdä Windows-verkon toimialuepalvelin (domain controller). Samban etuihin kuuluu myös se, että sille on saatavilla useita eri graafisia ohjelmia, joiden avulla sen konfigurointi on helpompaa.

Käyttöjärjestelmän sekä tarvittavien ohjelmistojen asennuksen jälkeen järjestelmä tulee konfiguroida kuntoon, jotta jaot toimisivat ja järjestelmässä olisi tietoturva kunnossa. Yrityskäytössä ja varsinkin ympäristöissä kuten Laurean turvalabra tulee olla erityisen tarkka tietoturva asioissa, etteivät oikeudettomat ihmiset pääse käsiksi heille kuulumattomaan tietoon. Järjestelmästä tulee laittaa palomuuriasetukset kuntoon, esimerkiksi iptables työkalulla, sekä määrittää käyttöoikeudet kuntoon.

Palvelimissa yksi ylläpidon kannalta erittäin tärkeä toiminto on, että järjestelmä tallentaa automaattisesti tärkeitä tietoja onnistuneista ja epäonnistuneista tapahtumista erillisiin lokitiedostoihin. Lokitiedostoista voi virhetilanteiden jälkeen tarkastella mikä on mennyt vikaan, tai selvitellä muuten tärkeitä tietoja. Lokitietoja voi tarkastella tiedosto kerrallaan, mutta on myös olemassa erillisiä ohjelmia, jotka keräävät automaattisesti tietoja Linuxin useista eri lokeista. Yksi tällainen ohjelma on LogWatch. Laurean turvalabran tapauksessa ongelmaksi saattaa muodostua se, että käsiteltävien tiedostojen käytöstä on jäätävä tarkat jäljet lokiin, jotta kaikki tiettyyn asiakirjaan tutustuneet voidaan jälkeenpäin selvittää. Linux taas ei automaattisesti välttämättä tallenna lokiin tarpeeksi tarkkoja tietoja. Siinä tapauksessa järjestelmään tarvittaisiin jokin erityinen loki-ohjelma taustalle pyörimään.

Jos Linuxin käytöstä ei ole paljoa kokemusta, niin yksi hyvä Linux-jakelu tiedostopalvelimelle olisi helppokäyttöinen Ubuntu Linux. Debianiin pohjautuvan Ubuntun LTS(Long-Term Support) versioille luvataan tukea ja turvapäivityksiä 3-5 vuotta, kun joissain jakeluissa tuki luvataan vain 18 kuukauden ajaksi. (Esittely 2009). Tiedostojen jakoon on suositeltavampaa käyttää Sambaa NFS:n sijaan, jos verkossa on Windows-koneita, tai on mahdollista, että jossain vaiheessa verkkoon tulee Windows-koneita. Samba on myös jossain määrin helppokäyttöisempi kuin NFS.

7 Yhteenveto tutkimuksesta

Työssä on tutkittu Laurean turvalabraa turvallisuusluokittelun näkökulmasta silmällä pitäen asioita, jotka tulee ottaa huomioon suunnittelussa. Työn alussa käytiin läpi työn tausta, jonka jälkeen kerrottiin käytetyistä tutkimusmenetelmistä. Työn suurin ja keskeisin osio oli turvallisuusluokittelu ja etenkin turvallisuusluokka II, jossa käytiin tarkkaan läpi, mitä nämä pitävät sisällään ja mitä vaatimuksia ne asettavat. Luvussa nimeltä ”Verkon rakentaminen” käsitellään edelliseen lukuun viitaten keinoja ja vaihtoehtoja, joilla voidaan toteuttaa turvallisuusluokittelun mukaisia ratkaisuja. Linux-luvussa selvitetään Linuxin ja muiden avoimen lähdekoodin ohjelmistojen tarjoamia mahdollisuuksia turvalabran kaltaisille projekteille.

7.1 Arviointi

Turvallisuusluokitellun tietoaineiston käsittelystä on säädetty erittäin tarkat määritykset, joiden puitteissa tulee toimia. Säännöissä määritellään erittäin kaikki tarvittavat vaatimukset sekä toimenpiteet asiakirjan koko elinkaaresta, luomisesta tuhoamiseen. Myös tilan, jossa käsitellään luokiteltua materiaalia, sekä tilassa olevien työasemien, palvelimien ja verkkojen tulee tukea niitä vaatimuksia, jotka turvallisuusluokittelu asettaa turvaluokitellun materiaalin käsittelyyn. Tästä syystä tuleekin edellä mainitun kaltaisen tilan suunnitteluun käyttää tarpeeksi aikaa ja suunnittelussa tulee ottaa huomioon kaikki yksityiskohdat.

Vaikka tilan suunnittelussa tulee olla erityisen tarkka ja käydä läpi kohta kohdalta, että tilasta tulee määritysten mukainen, on suurin huomio laitettava siihen hetkeen kun tila on valmis ja päivittäisessä käytössä. Päivittäisessä toiminnassa tulee nimittäin olemaan suurin riski, että laiminlyödään sääntöjä. Henkilökunnan kouluttamiseen ja ohjeistamiseen turvallisuusluokittelun kannalta tulee kiinnittää paljon huomiota. Koska ihminen on yleensä tietoturvassa heikoin lenkki, tulee tilassa työskentelevälle henkilökunnalle tehdä erityisen selväksi, minkälaisia vaatimuksia turvallisuusluokka II:n mukainen luokitus käyttäjille asettaa. Tulisi myös valvoa, että henkilökunta käyttäytyy turvaluokittelun vaatiman tietoturvan vaatimusten mukaan.

Linux ja vapaat ohjelmat tarjoavat paljon kustannustehokkaita valmiita työkaluja ja ohjelmia, joilla on helppoa toteuttaa yksinkertaisia tai monimutkaisempia työasemaympäristöjä

palvelimineen. Vapaita ohjelmia käytettäessä tulee kuitenkin ottaa huomioon, että ilmainen ei välttämättä aina ole ilmaista. Ohjelmistojen hankintahinnassa saavutettu etu voidaan helposti hävitä, jos osaaminen on puutteellista tai ohjelman ylläpito vaatii liikaa työtä. Esimerkiksi jos järjestelmän ylläpitoon tai koulutukseen tai muuhun vastaavaan tarvitaan jatkuvasti kallista ulkoista asiantuntija-apua, saattaa alun perin ilmaisen ohjelman käyttö tulla yhtä kalliiksi tai jopa kalliimmaksi kuin maksullisen ohjelman käyttö. Ulkopuolista asiantuntija-apua voidaan myös pitää tietoturvariskinä tämänkaltaisessa ympäristössä. Tästä syystä joissain tapauksissa maksullisten sovellusten käyttö voi olla suositeltavampaa kuin ilmaisten ohjelmien.

7.2 Tulokset

Tutkimuksen pääosa eli turvallisuusluokitusten selvitys onnistui hyvin, sillä työssä selvitettiin tarkasti turvallisuusluokittelu II:n vaatimukset. Työssä on esitetty keinoja joilla saa vaatimukset täytettyä niiltä osin kuin ne ovat tilan ja verkon kannalta olennaisia. Linux-osuudessa tutkimusta olisi helpottanut huomattavasti, jos käytettävissä olisi ollut jonkinlainen testiympäristö, jossa olisi ollut esimerkiksi pieni verkko, jossa olisi ollut Linux-tiedostopalvelin ja työasema. Testiympäristö olisi erityisesti helpottanut ja mahdollistanut tarkempaa tutkimusta Linuxin lokeista ja ohjelmista, jotka lokeja kirjoittavat ja jotka helpottavat lokien selailua. Vaikka työtä varten olisinkin voinut rakentaa testiympäristön, päätin luopua ajatuksesta koska osuus oli niin pieni osa työtä, ettei sen suuruinen työmäärä olisi ollut kannattavaa. Työn jonkinlaisena epäonnistumisena voisi pitää työn etenemistä, joka ei pysynyt lähellekään aikataulussa.

Lähteet

Kirjallisia lähteitä:

Barkakati, N. 2006. Linux All – In – One Desk Refrence For Dummies. Indiana: Wiley Publishing, Inc.
Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Jyväskylä: Docendo.
Järvinen P. & A. 2004. Tutkimustyön metodeista. Tampere: Opinpaja.
King, R., 2003. Mastering Active Directory for Windows Server 2003. San Francisco. Sybex.
Kuutti, W. & Rantala, A. 2007. Linux. Porvoo: Docendo.
MikroBitti 6/2009. Suomen suurin uusimman tekniikan lehti. Sanoma Magazines.

Elektroniset lähteet:

Avoin ohjelmakoodi valtaa pankkeja Brasiliassa. 2004. Digitoday. Viitattu 24.10.2008
http://m.digitoday.fi/?page=showSingleNews&newsID=200410767

Blancco File Shredder. 2009. Blancco. Viitattu 18.10.2009
http://www.blancco.com/fi/tuotteet+palvelut/blancco+file+shredder/yleista/

Ccleaner. 2009. Piriform. Viitattu 18.10.2009
http://www.ccleaner.com/

China's largest bank switches to Linux. 2005. computing.co.uk. Viitattu 24.10.2008
http://www.computing.co.uk/vnunet/news/2127256/china-largest-bank-switches-linux

Eraser. 2009. The Eraser Team. Viitattu 18.10.2009
http://eraser.heidi.ie/index.php#download

Esittely. 2009. Ubuntu Suomi. Viitattu 12.8.2009
http://wiki.ubuntu-fi.org/Esittely

Howto Delete Files Permanently and Securely in Linux. 2009. Techthrob.com. Viitattu 18.10.2009
http://www.techthrob.com/2009/03/02/howto-delete-files-permanently-and-securely-in-linux/

Langattomien lähiverkkojen (WLAN) turvallisuus. 2008 cert-fi. Viitattu 27.4.2009
http://www.cert.fi/ohjeet/2002/P_6.html

LaureaSID Labs. 2009. Laurea-ammattikorkeakoulu. Viitattu 14.2.2009.
http://www.laureasid.com/Default.aspx?TabId=83&language=fi-FI

LaureaSID. 2009. Laurea-ammattikorkeakoulu. Viitattu 14.2.2009.
http://www.laureasid.com/FrontPage/AboutLaurea/Prospectivestudents/tabid/82/language/fi-FI/Default.aspx

Laureasta koulutuksen laatuyksikkö 2008 – 2009. 2008. Laurea-ammattikorkeakoulu. Viitattu 14.2.2009.
http://www.laurea.fi/internet/fi/03_tietoa_laureasta/02/06_Uutiset/98_2008/Laureasta_koulutuksen_laatuyksikko_2008___2009/index.jsp

Linux valtaa Wall Streetiä. 2008. Tietoviikko. Viitattu 24.10.2008.
http://www.tietoviikko.fi/kaikki_uutiset/article138259.ece

NFS. 2009. opensuse.fi. Viitattu 12.8.2009
http://opensuse.fi/NFS

Tietoaineistojen turvallinen käsittely. 2008. Valtiovarainministeriö. Viitattu 2.3.2009
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/TietoaineistojenTurvallinenKasittely_v14.pdf

Työajanseurannan yhdistäminen kulunvalvontaan. 2005. Tamtron Solution Oy. Viitattu 27.4.2009
http://www.tyoajanseuranta.fi/kulunvalvontaanyhdistaminen.htm

Valtioneuvoston asetus tietoturvallisuudesta valtiohallinnossa. 2008. Valtiovarainministeriö Viitattu 2.3.2009
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20070717Lausun/02_Asetusluonnos_24_10_2008.pdf

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. 2009. Valtiovarainministeriö. Viitattu 2.3.2009
http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/01_tietoturvaryhma_VAHTI/index.jsp

What is Samba. 2009. The Samba Team. Viitattu 12.8.2009
http://us3.samba.org/samba/what_is_samba.html

Kuvat